

明 細 書

個人認証装置、及び個人認証装置を備えるシステム

技術分野

- [0001] 本発明は、本人であることを認証する個人認証装置、及びこの個人認証に基づいて所定の動作を許容するシステムに関する。

背景技術

- [0002] 個人認証を行う方法として、人の指紋、虹彩、眼底、顔の形状、手の血管走行の形状等の生体を用いて行う生体認証方法（バイオメトリクス方法）、磁気カードやICカードの記録媒体に記録した認証コードを用いる方法など種々の方法が知られている。
- [0003] 生体を用いる生体認証方法による装置では、生体データをセンサで検出し、予め登録しておいたデータと比較し、両者が一致するときに本人であると認証する。この認証装置では、生体データが個人差や測定条件により変動するため、高い検出精度を得ることが困難であり、検出精度を高めるには高精度のセンサを必要とし、また比較のために登録しておく生体データのデータ量も多く必要となるため、データ処理を行うためにサーバ側に生体データを記録しておくなどシステム装置構成も複雑となり、簡易な構成で低コストとすることができないという問題がある。
- [0004] また、磁気カードやICカードの記録媒体を用いる認証装置では、プラスチック製のカード上に設けた磁気材料やICチップに個人を特定するための認証データを記録しておき、利用者はこのカードを常に携帯し、個人認証を要する場所においてこのカードを検出装置で読み取らせる。この認証装置では、利用者はカードを常に携帯しなければならない、携帯し忘れた場合には個人認証を行うことができないという問題がある。他、カードが盗難された場合には、本人以外の第3者が本人になりすまして個人認証を行うことができるという問題もある。
- [0005] また、生体認証とカードを用いた認証とを組み合わせた個人認証も提案されている（例えば、特許文献1参照）。図22は生体認証とカードを用いた認証とを組み合わせた個人認証装置を説明するための概略図である。この個人認証装置101は、被認証者100の指の指紋を検出する指紋センサ101aと、カード102上に設けた記録媒体1

02aを読み取るカード読み取り手段101bとを備え、指紋センサ101aで検出した指紋100aの指紋データと、カード読み取り手段101bで記録媒体102aから取り込んだ指紋データとを照合することにより個人認証を行う。

特許文献1:特開2002-83289号公報

発明の開示

発明が解決しようとする課題

- [0006] 上記した生体認証とカード認証とを組み合わせた個人認証装置では、個人認証データを管理するサーバを不要とすることができ、また、カード盗難によるなりすましの問題を解決することができる。しかしながら、被認証者はカードを常に携帯しなければならない、カードを携帯し忘れた場合には個人認証を行うことができないという問題は依然として残っている。
- [0007] また、被認証者は本人であることを認証するには、携帯したカード102に登録した指紋データと同じ指紋100aの指100を指紋センサ101aに位置合わせさせることにより指紋データを取得させると共に、カード102をカード読み取り手段101bに位置合わせさせることにより認証用指紋データを取得させる必要がある。
- [0008] したがって、被認証者は指紋照合を行うために、指紋データの読み取りとカードからの認証用指紋データの取得とをそれぞれ別の二つの操作により行う必要があり、個人認証装置の操作性は良好なものとは言い難いという問題がある。
- [0009] そこで、本発明は前記した従来の問題点を解決し、指紋データの読み取りと記録媒体からの認証用指紋データの取得とを一操作で行うことができることを目的とする。

課題を解決するための手段

- [0010] 本発明は、個人認証装置と、この個人認証装置を備え、本人認証に基づいて動作を行うシステムに関する。
- [0011] 本発明の第1態様は個人認証装置であり、指紋を検出する指紋センサと、被認証者の指又は手首あるいは足首に携帯する携帯装置に搭載される記憶媒体を呼び出し、その記憶媒体に格納される記録情報を読み出すスキャナとを装置本体に一体に備え、さらに、指紋センサで検出した被認証者の指の指紋データと、スキャナにより被認証者の指又は手首あるいは足首に装着された携帯装置の記録媒体から読み出し

た指紋照合用データとを照合する指紋照合手段とを備える。指紋照合手段は、指紋データと指紋照合用データとの一致に基づいて記録媒体の所持者が本人であることを認証する。

- [0012] 本発明の個人認証装置は、指紋センサとスキャナとが装置本体に一体に備える構成とすることにより、指紋センサによる被認証者の指紋データの取得と、スキャナによる被認証者の指又は手首あるいは足首に装着された携帯装置の記録媒体に格納されている指紋照合用データの読み出しを、被認証者は装置本体に対して一つの操作を行うだけで同時に行うことができる。
- [0013] 携帯装置は、指輪状形状又は腕輪状形状とし、被認証者の指又は手首あるいは足首に装着することができ常時携帯が可能であると共に、指紋の検出と同時に携帯装置に設けられた記録媒体に格納された指紋照合用データ等の情報を読み出すことができる。
- [0014] 個人認証装置の装置本体上において、指紋センサとスキャナは、指紋センサによる被認証者の検出対象の指紋検出と、被認証者が携帯する携帯装置に搭載される記録媒体の読み出しとを同時に行うことができる位置に配置する。例えば、指輪状形状の携帯装置を用いる場合には、指紋センサは被認証者の指の指紋を検出し、スキャナはその指に装着された指輪状形状の携帯装置に設けられた記録媒体を読み出す。なお、指輪状形状の携帯装置は、指紋検出を行う指に装着される必要はなく、スキャナの検出範囲内であれば任意の指に装着することができる。
- [0015] また、本発明の携帯装置を装着する指は、手の指あるいは足の指のいずれとしてもよい。例えば、手の指に適用する場合には、記録媒体を装着する手の指の指紋照合用データを記録しておき、手の指の指紋を指紋センサで検出して得た指紋データと指紋照合用データとを照合することで認証を行う。また、足の指に適用する場合においても同様に、記録媒体を装着する足の指の指紋照合用データを記録しておき、足の指の指紋を指紋センサで検出して得た指紋データと指紋照合用データとを照合することで認証を行う。
- [0016] 特に、足の指に指輪状形状の携帯装置を装着する場合には、一般に足の指は指先の方が付け根よりも太いため、手の指に装着する場合よりもはずれ落ちるといった

不都合が少ないという効果がある。

- [0017] また、腕輪状形状の携帯装置を用いる場合には、指紋センサは被認証者の指の指紋を検出し、スキャナはその指紋検出を行う手の手首や足首に装着された腕輪状形状の携帯装置に設けられた記録媒体を読み出す。
- [0018] 指紋センサとスキャナは、指紋検出と記録媒体からの読み出しとを同じ指あるいは同じ手に対する操作で行うことができるため、カードを用いた認証のように、指紋検出とカード読み出しの2つの操作を不要であり一操作で済ますことができる。
- [0019] また、装置本体は表示手段を備えた構成とすることができ、指紋照合により本人と確認された場合には、スキャナは記憶媒体に格納される記録情報を読み取って表示手段に表示することができる。
- [0020] また、本発明の個人認証装置は、指紋照合に基づいて、スキャナは記憶媒体に格納される記録情報から個人を特定する識別データを読み取って外部サーバに送り、外部サーバから識別データで特定される個人情報を取り込むこともできる。
- [0021] また、本発明の個人認証装置は、指紋照合に基づいて、指紋センサが検出した指紋データを外部サーバに送り、外部サーバから指紋データで特定される個人情報を取り込むこともできる。
- [0022] 本発明の第2の態様は個人認証装置を備えるシステムである。
- [0023] 第2の態様のシステムの第1の形態は、押印やサインの処理に適用した形態であり、個人認証装置と、印章データを出力する電子押印装置とを備えた構成である。個人認証装置は、指紋照合に基づいて、スキャナにより憶媒体に格納される記録情報から印章データを読み取って電子押印装置に送る。電子押印装置は、スキャナで読み取られて送られた印章データを外部装置に対して書き込むと共に、その外部装置から書き込んだ印章データを読み出すことができる。
- [0024] また、装置本体に表示手段を設け、記録媒体から読み取った印章データ及び／又は外部装置から読み出した印章データを表示して確認することができる。
- [0025] 第1の形態の電子押印によれば、サーバ等に印章データを格納する必要がなく、また、操作時においてもサーバにアクセスする必要がないため、簡易な構成及び簡易な操作で押印を行うことができる。

- [0026] 第2の形態は、錠の開閉に適用した形態であり、個人認証装置と、認証データの照合により解錠する錠装置とを備えた構成である。個人認証装置は、指紋照合に基づいて、スキャナにより記憶媒体に格納される記録情報から認証データを読み取って錠装置に送る。錠装置は、スキャナで読み取られて送られた認証データと予め記憶する認証データとの照合により解錠する。
- [0027] 第2の形態の錠装置によれば、解錠のための鍵やカードが不要であり、指紋データの取得と同時に記録媒体から認証データを取得することができ、この認証データにより解錠することができ、解錠時においてサーバにアクセスする必要がないため、簡易な構成及び簡易な操作で解錠することができる。
- [0028] 第2の態様のシステムによれば、第1の態様の個人認証装置を備えることにより、個人認証に基づく処理を簡易な構成で行うことができる。

発明の効果

- [0029] 以上説明したように、本発明によれば、指紋データの読み取りと記録媒体からの認証用指紋データの取得とを一操作で行うことができる。

図面の簡単な説明

- [0030] [図1]本発明の個人認証装置の構成を説明するための概略図である。
- [図2]本発明の個人認証装置の指紋センサとスキャナとの位置関係、及び被認証者による操作を説明するための概略図である。
- [図3]本発明の個人認証装置による個人認証、及び個人認証に基づく処理の動作例を説明するための概略図である。
- [図4]本発明の個人認証装置と利用者及び外部装置との間の信号関係を説明するための図である。
- [図5]本発明の個人認証装置の錠装置への適用例を説明するために図である。
- [図6]本発明の個人認証装置と利用者及び電子印章装置との間の信号関係を説明するための図である。
- [図7]本発明の個人認証装置の電子印章装置への適用例を説明するための図である。
- [図8]本発明の個人認証による情報照会処理を説明するための図である。

[図9]本発明の個人認証装置における指紋センサとスキャナとの関係を示す図である。

[図10]本発明の個人認証装置に用いる指輪状形状ないし腕輪状形状の携帯装置の構成を説明する図である。

[図11]本発明の携帯装置が備える記録媒体の構成例を説明するための図である。

[図12]本発明の記録媒体の帯状部材にアンテナを設ける構成例を説明するための図である。

[図13]本発明の記録媒体の帯状部材にアンテナを設ける構成例を説明するための図である。

[図14]本発明の個人認証装置の医療分野における各段階での適用例を説明するための図である。

[図15]本発明の個人認証装置の診察段階での利用を説明するための図である。

[図16]本発明の個人認証装置の診察段階での利用を説明するための図である。

[図17]本発明の個人認証装置の投薬、処置段階での利用を説明するための図である。

[図18]本発明の個人認証装置の調剤段階での利用を説明するための図である。

[図19]本発明の個人認証装置の薬剤の窓口での受け渡し段階での利用を説明するための図である。

[図20]本発明の個人認証装置の薬剤の受け取り段階での利用を説明するための図である。

[図21]本発明の個人認証装置の診療に関わる履歴を用いた本人認証を説明するための図である。

[図22]生体認証とカードを用いた認証とを組み合わせた個人認証装置を説明するための概略図である。

符号の説明

[0031] 1…個人認証装置

1a…指紋センサ

1b…スキャナ

1c…指紋照合手段
1d…記録手段
1e…出力手段
1f…表示手段
1g…コード管理手段
1h…出力手段
1i…入出力手段
1j…入力手段
1k…照合手段
1f…表示手段
2…記録媒体
2a…媒体チップ
2b…回路パターン
2c…回路基板
2d…コンデンサ
2e…アンテナ
3…携帯装置
3a…帯状部材
3b…凹凸部
3c…環状部材
3d…開口部
3e…アンテナ
10…外部装置
11…電子印章装置
12…錠装置
20…サーバ
20a…一時コード発行管理装置
20b…コード発行管理装置

20c…一時コード管理装置

20d…履歴管理装置

30…情報処理装置

40…扉

50…用紙

51…記録媒体

60…円筒体

70…ドア

71…ドアノブ

100…指

100a…指紋

101…個人認証装置

101a…指紋センサ

101b…カード読み取り装置

102…カード

102a…記録媒体

110…診察段階

120…投薬, 処置段階

121…薬剤

130…調剤段階

131…薬剤

140…受け渡し段階

150…薬剤の受け取り段階

発明を実施するための最良の形態

[0032] 以下、本発明の実施の形態について、図を参照しながら詳細に説明する。

[0033] 図1ー図4を用いて本発明の個人認証装置の構成及びその処理を説明し、図4, 5を用いて本発明の個人認証による解錠処理を説明し、図6, 7を用いて本発明の個人認証による電子印章処理を説明し、図8を用いて本発明の個人認証による情報照

会処理を説明する。また、図9を用いて本発明の個人認証装置における指紋センサとスキャナとの関係をし、図10を用いて本発明の個人認証装置に用いる指輪状形状ないし腕輪状形状の携帯装置の構成を説明する。

[0034] 図1は個人認証装置の構成を説明するための概略図である。図1において、個人認証装置1は指紋センサ1aとスキャナ1bを備える。指紋センサ1aは、被認証者の指100の指紋を検出する。スキャナ1bは、被認証者の指100あるいは手首や足首に携帯される携帯装置3に搭載される記憶媒体2を呼び出し、この記憶媒体2に格納される記録情報を読み出す。指紋センサ1aとスキャナ1bは、個人認証装置1の装置本体に一体に設けられる。

[0035] 個人認証装置1は、指紋照合により記録媒体3の所持者と本人との同一性を認証する指紋照合手段1cを備える。指紋照合手段1cは、指紋センサ1aで検出した被認証者の指の指紋データと、スキャナ1bにより携帯装置3の記録媒体2から読み出した指紋照合用データとの照合を行う。指紋照合手段1cによる指紋照合は、例えば検出した指紋データから指紋の特徴点を抽出し、指紋照合用データの特徴点との一致を判定することにより行うことができる。

[0036] なお、図1に示す構成例では、指紋センサ1aで検出した指紋データを指紋照合手段1cに直接入力する構成を示しているが、指紋センサ1aにより指紋を走査して行う指紋データの検出において検出時間を要する場合には、指紋センサ1aが検出する指紋データを記憶手段1dに逐次記憶し、全ての指紋データが検出された後、指紋照合手段1cに送って指紋照合の処理を行う構成としてもよい。

[0037] 指紋照合手段1cによる照合結果は、出力手段1eにより外部装置10に出力する他、装置本体に設けた表示手段1fに表示することができる。

[0038] 一方、記憶媒体2は、例えば無線タグやICチップ等と呼称される記録と通信の両機能を備える素子であり、メモリ機能、外部との通信機能、外部から得られる誘導電波により駆動電流を形成する駆動機能等を備える。メモリ機能は、指紋照合用データを記録する他、被認証者を識別する識別データ、各被認証者の生体データや電子押印等に用いる印章データ等の個人情報、錠装置の解錠に用いる認証データ等の種々のデータを予め登録して記録しておく。

- [0039] 個人認証装置1は、この記録媒体2に記録される記録情報を取得するための機能を備える。この機能は、例えば、記録媒体3に対して誘導電波を送って記録媒体3を駆動させ、スキャナIDを記録媒体3に送る。記録媒体3は、誘導電波で誘起された電流により駆動し、送られたスキャナIDを登録してあるスキャナIDと照合し、一致した場合には指紋照合用データを個人認証装置1に送信する。なお、スキャナIDによるスキャナの照合は省略することもできる。
- [0040] 個人認証装置1のスキャナ1bは、記録媒体3から送信された指紋照合用データの他に、識別データ、個人情報、認証データ等の種々のデータを受信する。スキャナ1bで読み取ったこれらの各種データは記録手段1dに記憶することができる。なお、これら個人情報や認証データ等については、指紋照合用データによって指紋照合を行い、指紋データの照合が確認された後に記憶媒体2からの読み取りを開始するようにしてもよい。
- [0041] 本発明の個人認証装置1が備える指紋センサ1aとスキャナ1bは、装置本体に対して一体で設けられ、被認証者が装置本体に対して行う一認証操作により、指紋センサ1aによる指紋検出と、スキャナ1bによる記録媒体2からの指紋照合用データの読み取りとを同時に行うことができ、指紋検出の操作と指紋照合用データを読み取る操作を別に行うことなく、一つの操作で行うことができる。
- [0042] 図2は指紋センサとスキャナとの位置関係、及び被認証者による操作を説明するための概略図である。ここで、被認証者は記録媒体2を搭載した携帯装置3を自身の指100に装着しているものとする。携帯装置3は指輪状の形状であり、被認証者の指100に常時装着しておくことができる。
- [0043] 指紋センサ1aは、個人認証装置1の装置本体においてその外壁部分にセンサ面が露出するように設ける。被認証者は、指紋部分をセンサ面に接触させることにより指紋検出を行う。なお、指紋センサは任意の検出形態のものを適用することができる。
- [0044] 一方、スキャナ1bは、同装置本体において指紋センサ1aの近傍に設ける。指紋センサ1aを設置する位置は、被認証者が自身の指紋部分を指紋センサ1aに接触させて指紋検出を行う際に、指100に装着した携帯装置3の記録媒体2がその通信可能

な範囲内となるように設定する。これによって、被認証者が指紋認証を行うために自身の指紋を指紋センサ1aに接触させると(図2(b))、スキャナ1bは記録媒体2を通信可能な範囲内となるため、被認証者は指を指紋検出の位置としたままで、記録媒体から認証用指紋データなどの記録情報を読み取ることができる。

[0045] なお、スキャナ1bの読み取り距離の範囲を広く設定した場合には、スキャナ1bは図2に示すように携帯装置3と一致する設置する必要はなく、通信が可能な範囲内であれば、スキャナ1bと携帯装置3との間に距離が生じる構成とすることもできる。これによれば、指紋を検出する指と異なる指に携帯装置3を装着させることもできる。

[0046] 図3は、本発明の個人認証装置による個人認証、及び個人認証に基づく処理の動作例を説明するための概略図である。

[0047] ここで、携帯装置3に搭載される記録媒体2は、指紋照合用データの他に、個人を識別する識別データ、各個人が固有に備える個人情報、外部装置10との間で一対一の関係を特定して認証する認証データ等を予め登録して記録している。本人認証は、指紋センサ1aにより被認証者の指紋100aを検出して取得した指紋データと、スキャナ1bにより記録媒体3から読み出して取得した指紋照合用データと照合して行う。

[0048] 指紋照合の照合結果は表示手段に表示する他(図中の破線A)、外部装置10やサーバ20に送って使用することもできる。外部装置10としては、例えば、電子押印装置11や錠装置12とすることができる。

[0049] 電子押印装置11は、押印あるいはサインの操作を電子的に行うものであり、予め記録しておいた印章データを書類に搭載した記録手段に送ることにより、押印あるいはサインの操作の代わりとするものである。また、錠装置12は、金庫、ロッカー、ドアなどの施錠、解錠を電氣的に行うものであり、解錠は予め登録しておいた認証データの認証することにより行う。

[0050] 印章データは、例えば記録媒体2の個人情報内に格納しておくことができ、また、認証データは、例えば記録媒体2内に格納しておくことができる。これらの印章データ及び認証データは、指紋照合データと共に読み出すことも、あるいは、指紋照合が済んだ後に読み出すこともできる。

- [0051] 指紋照合が済んだ後に読み出す場合には、図3中の破線Bに示すように、指紋照合に基づいて、記録媒体2に格納される印章データあるいは認証データを読み出し、読み出したデータを電子押印装置11や錠装置12等の外部装置10に送信する。このように、指紋照合に基づいて印章データあるいは認証データを読み出すことにより、押印や解錠の処理の安全性を高めることができる。
- [0052] また、個人認証装置1はサーバ20に接続することにより、より正確な本人認証を行ったり、他の情報処理装置の被認証者の情報を送ることができる。サーバ20は、被認証者を特定する識別データ、被認証者のより詳細な指紋照合用データ、及び個人情報をデータベースに備え、個人認証装置1から送られた指紋データをより詳細な指紋照合用データと照合することにより、本人認証の確度を高めることができる。また、サーバ20では、手段指紋照合に加えて、識別データの照合により本人認証を行うこともできる。
- [0053] また、サーバ20は、本人認証を受けて(図中の破線C)、識別データや個人情報を他の情報処理装置30に送信することができる。情報処理装置30は、例えば医療機関や公共機関等が備えることができ、サーバ20で管理する生体データや住所、氏名、生年月日等の個人情報を取り込むことができる。
- [0054] 図4は、個人認証装置と利用者及び外部装置との間の信号関係を説明するための図であり、図5の構成例と共に外部装置として錠装置に送信する例について説明する。なお、以下に付す番号は図中の番号と対応して示している。
- [0055] はじめに、個人認証装置1のスキャナ1bは、利用者が装着する携帯装置3に搭載される記録媒体2に対して誘導電波を発すると共に、発信元のスキャナを識別するスキャナIDを発信する(1)。被認証者が携帯する携帯装置3に搭載される記録媒体2は、この誘導電波により駆動電流を得て駆動し、受信したスキャナIDと予め記憶しておいたスキャナIDとを照合する。登録されたスキャナIDであれば、予め登録しておいた被認証者の指紋データを指紋照合用データとして個人認証装置1に送信する。この指紋照合用データは暗号化して送信することができる。
- [0056] 発信元のスキャナIDが登録されていない場合には、応答を行わないか、あるいは未登録のスキャナIDであることを返信する。なお、スキャナIDの照合処理を省き、指

紋照合用データの要求に基づいて暗号化した指紋照合用データを送信する形態とすることもできる(2)。

[0057] 個人認証装置1のスキャナ1bは暗号化された指紋照合用データを受信し(3)、復号して指紋照合用データを取得する(4)。一方、個人認証装置1の指紋センサ1aは被認証者の指紋を検出し(5、6)、指紋データを取得する(7)。

[0058] 指紋照合手段1cは、取得した指紋照合用データと指紋データとの照合を行う。この指紋照合は、例えば、指紋データから予め設定しておいた特徴点を抽出し、その特徴点が指紋照合用データ中の特徴点と一致するかを判定することにより行う。本発明の個人認証装置1では、この指紋照合に用いる指紋照合用データを被認証者が装着する携帯装置に搭載した記録媒体から取得するため、装置本体に予め登録しておいたり、サーバに問い合わせるといった指紋照合用データの管理の手間を省くことができ、システムを簡略化することができる(8)。

[0059] 指紋照合により本人認証が確認されると、外部装置に本人認証を確認した信号を形成し(9)送信する(10)。外部装置はこの本人認証の確認信号を受信し、所定の処理を行う(11)。

[0060] 図4中の下方に示す一点鎖線で囲む処理は、外部装置として錠装置に適用した例を示している。

[0061] 指紋照合手段1cは、取得した指紋照合用データと指紋データとの照合を行い(12)、本人認証が確認された場合には、錠装置12を解錠するための認証データの読み出しを行う。この認証データは、錠装置12を解錠する鍵として使用するものであり、各錠装置12毎に登録された利用者に対して割り当てられ、記録媒体2に予め記憶しておくものとする。

[0062] 個人認証装置1は、スキャナ1bと記録媒体2との間の通信により、記録媒体2に登録されている認証データを取得し(13-15)、取得した認証データを外部装置の錠装置12に送信する(16)。錠装置12は認証データを受信し(17)、この認証データと登録しておいた認証データとを照合する(18)。認証データが一致した場合には、錠装置12を解錠する(19)。なお、認証データは暗号化しておき、外部装置側で復号して照合することにより、外部装置側のセキュリティを高めることができる。

- [0063] 図5は、本発明の個人認証装置の錠装置への適用例であり、金庫やドアやロッカー等の扉に用いる例を示している。図5に示す例では、扉40に本発明の個人認証装置1を設け、個人認証装置1で取得した認証データを錠装置12に送る構成としている。個人認証装置1は扉40の任意の位置に設けることができるが、例えば扉10の取っ手部分に近接した位置に設けることにより、指紋センサによる指紋データの取得と、スキャナによる指紋照合用データ及び認証データの取得と、扉40の開放動作とを一連の操作により行うことができる。
- [0064] カードを用いて本人認証を行い、その本人認証に基づいて解錠を行って扉を開ける構成では、カードをカード読み取り装置に読み取らせる操作と、扉を開放する操作の少なくとも2つの操作を要するのに対して、本発明の個人認証装置を適用したシステムによれば、カードを読み取らせる操作が不要であるため、本人認証を行う操作と同時に扉を開放する操作を行うことができる。
- [0065] 次に、外部装置を電子印章装置とした例について、図6, 7を用いて説明する。図6は個人認証装置と利用者及び電子印章装置との間の信号関係を説明するための図であり、図7は電子印章装置への適用例を説明するための図である。
- [0066] なお、以下に付す番号は図中の番号と対応して示している。
- [0067] はじめに、前記した図4中の(1)から(8)の工程と同様にして指紋データと指紋照合用データとを照合する。
- [0068] 指紋照合手段1cは、取得した指紋照合用データと指紋データとの照合を行い(8)、本人認証が確認された場合には、電子印章装置11で使用する電子印章データの読み出しを行う。この電子印章データは、電子印章装置11において電子的に押印を行うためのデータであり、例えば、押印を求める機関に送ったり、印紙や書類中に組み込んだ記録媒体にこの電子印章データを送って記録させることにより、押印と同等の処理を行うものである。この電子印章データは、各利用者毎に固有であり、記録媒体2に予め記憶しておく。記録媒体2に記憶された電子印章データは、本発明の個人認証装置1により必要に応じて読み出され、電子印章装置11により書き込み処理を行うことで押印あるいはサインに代わる処理を行う。
- [0069] 個人認証装置1は、指紋照合の後、スキャナ1bと記録媒体2との間の通信により、

記録媒体2に記録されている暗号化された電子印章データを取得する(20-22)。取得した電子印章データを復号し(23)、復号した電子印章データを電子印章装置11に送信する(24)。このとき、電子印章データを表示手段1fに表示することもできる。この電子印章データは、印章画像として表示することもできる(25)。

[0070] なお、上記した(20-22)の工程では、指紋照合に基づいて電子印章データを取得しているが、指紋照合の結果に関わらず電子印章データを記録媒体から取得しておき、指紋照合が確認された場合にのみ暗号化された電子印章データを復号するようにしてもよい。

[0071] 電子印章装置11は、個人認証装置1から送られた電子印章データを受信し(26)、この電子印章データを印紙や押印用紙等の書類等に組み込んでおいた無線タグ等の記録媒体に書き込み、記録する(27, 28)。電子印章装置11は、書き込んだ電子印章データを読み取って(29)、表示手段1fに表示する(30)。

[0072] 表示手段1fは、記録媒体2から読み出した電子印章データと、電子印章装置11で読み取った電子印章データとを並べて表示することにより、押印を確認することができる。

[0073] 図7は、本発明の個人認証装置を電子印章装置に適用した一例である。図7に示す例では、個人認証装置1を電子印章装置11とを接続する構成である。

[0074] 個人認証装置1は、前記したように、指紋センサ1aにより被認証者の指紋データを検出し、スキャナ1bにより携帯装置3に搭載した記録媒体2から指紋照合用データを読み取って本人認証を行い、本人認証に基づいて記録媒体2から電子印章データを取得する。

[0075] 個人認証装置1は、取得した電子印章データを電子印章装置11に送り、電子印章装置11により印紙や押印用紙等の用紙50に貼り付けておいた無線タグ等の記録媒体51に書き込み、書き込んだ電子印章データを読み取って個人認証装置1に送り返し、表示手段1fに表示する。

[0076] 個人認証装置1は、指紋センサによる指紋データの取得と、スキャナによる指紋照合用データ及び電子印章データの取得とを一つの操作により行うことができる。なお、電子印章装置11による押印操作は、電子印章装置本体に設けたスイッチにより行

うことができるが、この押印操作を単に押印時の確認とし、個人認証装置1において本人認証がされたことにより押印操作を行う構成とすることもできる。

- [0077] カードを用いて本人認証を行い、その本人認証に基づいて電子押印を行う構成では、カードをカード読み取り装置に読み取らせる操作と、電子押印を行う操作の少なくとも2つの操作を要するのに対して、本発明の個人認証装置を適用したシステムによれば、カードを読み取らせる操作が不要であるため、本人認証を行う操作と同時に電子押印の操作を行うことができる。
- [0078] 次に、本発明の個人認証装置による本人認証に基づいてサーバから情報を取得する例について、図8を用いて説明する。図8は、個人認証装置と利用者とサーバとの間の信号関係を説明するための図である。なお、以下に付す番号は図中の番号と対応して示している。
- [0079] はじめに、前記した図4中の(1)から(8)の工程と同様にして指紋データと指紋照合用データとを照合する。
- [0080] 指紋照合手段1cは、取得した指紋照合用データと指紋データとの照合を行い(8)、本人認証が確認された場合には、サーバから情報を取得するために本人を識別するための識別データの読み出しを行う。この識別データは、サーバ20において本人を識別するためのデータであり、サーバ20と利用者が携帯する携帯装置3に搭載する記録媒体2に登録し記録しておく。
- [0081] 記録媒体2に記憶されている識別データは、本発明の個人認証装置1により必要に応じて読み出され、この識別データによりサーバにおいて本人を確認し、情報を取得する。
- [0082] 個人認証装置1は、指紋照合の後、スキャナ1bと記録媒体2との間の通信により、記録媒体2に記録されている暗号化された識別データを取得する(40-42)。取得した識別データを復号する(43)。なお、上記した(40-42)の工程では、指紋照合に基づいて識別データを取得しているが、指紋照合の結果に関わらず識別データを記録媒体から取得しておき、指紋照合が確認された場合にのみ暗号化された識別データを復号するようにしてもよい。
- [0083] また、個人認証装置1は、指紋照合した後サーバ20のログインする(44)。サーバ2

0は、個人認証装置1からのログインを確認し(45)、暗号鍵を送信する(46)。個人認証装置1はサーバ20から送られた暗号鍵を復号し(47)、この暗号鍵を用いて取得しておいた識別データを暗号化し(48)、サーバ20に暗号化した識別データを送信する(49)。

[0084] サーバ20は、暗号化された識別データを受信し(50)、復号する(51)。識別データに基づいて利用者を特定し、記録している利用者の情報の内から要求された個人情報を読み出して暗号化し(52)、個人認証装置1に送る(53)。個人認証装置1は、暗号化された個人情報を受信して(54)復号し(55)、表示手段1fに表示する。

[0085] 本発明の個人認証装置1において、指紋センサ1aとスキャナ1bとの装置本体での配置は、図1、2で示した構成に限られるものではなく他の構成とすることもできる。図9は、個人認証装置の指紋センサとスキャナの他の配置構成を説明するための図である。

[0086] 図9(a)において、スキャナ1bは、被認証者が指先を指紋センサ1aに接触させたときに、被認証者が装着する携帯装置3に搭載される記録媒体2との間で通信可能な範囲であれば、装置本体の任意の位置に配置することもできる。

[0087] 図9(a)中のスキャナ1bは、通信距離を短くして、指紋センサ1aにより指紋検出を行う指に装着された指輪状の携帯装置3に搭載した記録媒体2のみから情報を取得する。

[0088] 図9(a)中のスキャナ1b'は、通信距離を長くして、指紋センサ1aにより指紋検出を行う指以外の指に装着された指輪状の携帯装置3、あるいは手首や足首に装着されたブレスレット状の携帯装置3に搭載した記録媒体2から情報を取得する。

[0089] 図9(b)は、円筒状部材60の外表面に指紋センサ1aを設け、内部にスキャナ1bを設ける構成の例である。この構成によれば、被認証者は円筒状部材60を握る操作により、本人認証を行うことができ、車やバイク等のハンドルに適用することができる。

[0090] 図9(c)は、ドア70のドアノブ71に適用した例であり、ドアノブ71の外表面に指紋センサ1aを設け、内部にスキャナ1bを設ける構成例である。この構成によれば、被認証者はドアノブ71を握る操作により、本人認証を行うことができる。

[0091] 次に、本発明の個人認証装置に用いた携帯装置の構成例について図10を用いて

説明する。携帯装置3は、利用者の指や手首や足首に装着する指輪状あるいは腕輪状の形状であり、輪の一部に記録媒体2が組み込まれる。

[0092] 携帯装置3は帯状部材3aと環状部材3cとからなり、この帯状部材3aを湾曲させ、その両端部を環状部材3cの各開口端部に挿入して固定することによりリング状に形成される。図10(a)は、帯状部材3aを環状部材3c内に挿入する前の状態を示している。

[0093] 帯状部材3a及び環状部材3cは樹脂製とし、環状部材3cは加熱により収縮する熱可塑性樹脂とする。携帯装置3は、帯状部材3aと環状部材3cとを組み合わせる構成とすることにより、利用者の指や手首や足首の太さに対応した大きさに形成することができる。

[0094] 輪状に形成するには、帯状部材3aを利用者の指や手首や足首の合わせた後、その両端を環状部材3cの開口部3d内に挿入し、挿入する長さを調整することにより輪の大きさを利用者の指や手首や足首の太さに合わせ(図10(b))、環状部材3cを加熱して収縮させ固定する(図10(c))。これにより、利用者の指や手首や足首の太さに対応した大きさに合わせることができる。

[0095] このとき、帯状部材3aの両端に溝等の凹凸部分を形成しておくことにより、環状部材3c内に挿入して固定した際に、帯状部材3aの端部と環状部材3cとの間の摩擦を大きくして、帯状部材3aの端部が環状部材3cから脱落することを防ぐことができる。また、帯状部材3aは、長さの異なるものを複数種用意しておくことにより、利用者の指や手首や足首の多種類の太さに対応することができる。

[0096] 以下、携帯装置3が備える記録媒体2の構成例について図11を用いて説明し、携帯装置の他の構成例について図12, 13を用いて説明する。

[0097] 図11において、携帯装置3が備える記録媒体2は、例えばICチップ等と呼ばれる媒体チップ2aと、この媒体チップ2aを駆動するための回路パターン2bと、媒体チップ2a及び回路パターン2bを構成する回路基板2cと、駆動用電源となるコンデンサ2dと、外部装置との間で行う送受信や電力供給のためのアンテナ2e等を備える。なお、コンデンサ2dは、外部装置からの高周波による電磁誘導によって、回路基板2c側が必要とする電力の供給を受ける。図11(b)は、これら各要素の一配置例を示している。

が、この配置に限られるものではない。また、図11(a)は、記録媒体2を環状部材3cに設けた例を示している。記録媒体2は、環状部材3cを形成する際に、環状部材3c内に一体で埋め込む他、形成した環状部材3cの表面に貼り付ける構成としてもよい。表面に貼り付ける構成の場合には、貼り付けた記録媒体2の外側表面を樹脂等でコーティングして保護膜を形成してもよい。

[0098] 記録媒体2は、図11(a)に示すように、携帯装置3の環状部材3cに設ける構成の他に別の構成としてもよい。図12, 13は、記録媒体を設置する別の構成の説明するための図である。

[0099] 記録媒体2が備えるアンテナ2eは、外部装置との間の送受信感度を高めるためには、長さや面積が大きいことが望ましい。

[0100] 図12, 13は、記録媒体2の帯状部材3aにアンテナ2eを設ける構成例である。なお、図12(a), 図13(a)は斜視図であり、図12(b), 図13(b)は断面図である。帯状部材3aは、内部にアンテナ2eを埋め込んで形成する他、帯状部材3aの表面に貼り付ける構成としてもよい。表面に貼り付ける構成の場合には、貼り付けたアンテナ3eの外側表面を樹脂等でコーティングして保護膜を形成してもよい。

[0101] なお、図12, 13に示す構成例の帯状部材3aは、一部を切り欠いた環状体により構成することができ、弾性を有する樹脂により形成することができる。この構成とすることによって、使用者の指や手首や足首の太さが異なる場合にも対応することができ、また、同一の使用者であっても体調によって指や手首や足首の太さが変化した場合にも対応することができる。

[0102] 図12に示す構成例は記録媒体2を帯状部材3aの周方向のほぼ中央部に設けた例であり、図13に示す構成例は記録媒体2を帯状部材3aの周方向の端部に設けた例であるが、記録媒体2は帯状部材3aの周方向のいずれの位置に設けても良い。

[0103] また、図12では、記録媒体2を帯状部材3aの外周面側に貼り付ける例を示しているが、内周面側に貼り付ける構成としてもよい。また、記録媒体2を帯状部材3a内に埋め込んで形成する構成としてもよい。

[0104] また、図13に示す構成例において、携帯装置3を指や手首や足首に装着する際に、アンテナ3eが設けられた帯状部材3aが個人認証装置のスクヤナと対向する位置に

装着することができる。この装着位置とした場合には、アンテナ3eとスキャナとの距離を短くすることができるため、送受信感度を高めることができる。また、アンテナ3eとスキャナとの間に指や手首や足首等の人体部分を挟まないため、人体による電波の吸収効果の影響を低減させることができ、送受信感度を高めることができる。

- [0105] 次に、本発明の個人認証装置を医療分野に適用した場合の例について、図14ー図21を用いて説明する。なお、図15ー図20は、医療分野において、医師による診察による投薬や処置の指示、前記医師に指示に基づく投薬や処置、前記医師に薬剤指示に基づく調剤、前記医師に薬剤指示に基づく薬剤の受け渡しや受け取り等の各段階での適用例を示し、図21は、医療分野において、利用者の履歴データを本人認証に利用する適用例を示している。
- [0106] 図14は、医療分野における各段階での適用例を示している。診療過程において、本発明は、医師による診察段階、投薬や処置の段階、調剤の段階、薬剤の配布段階等の各段階に適用することができる。なお、薬剤の配布段階は、薬剤を窓口等で受け渡す形態とする他、用意された薬剤を受け取る形態とすることができる。
- [0107] 上記診療過程の各段階(診察段階110、投薬、処置段階120、調剤段階130、薬剤の窓口での受け渡し段階140、薬剤の受け取り段階150)では、前記したように、各医療対象者が装着する記録媒体2を個人認証装置1で確認することで本人であることを認証する他、本発明の個人認証装置1を用いることによって、診察段階110で医師等が指定した投薬や処置を、他の各段階(投薬、処置段階120、調剤段階130、薬剤の配布段階(薬剤の窓口での受け渡し段階140、薬剤の受け取り段階150)において照合し確認することができる。これにより、本人の確認に加えて、指示した投薬や処置の確認を行うことができる。
- [0108] 以下、上記各段階について説明する。
- [0109] はじめに診察段階110について図15、16を用いて説明する。以下に示す例では、各診察行為に対して一時コードを設定し、この一時コードを用いて投薬や処置を特定する。この一時コードは、医師、医療対象者、診察で指定する投薬や処置等を特定する。
- [0110] 図15は、一時コードをサーバ20で発行し、医師等が使用する個人認証装置1に割

り振る。例えば、一時コードとしてT01, T02, T03, …, T11, T12, T13, …, T21, T22, T23, …, を発行し、これらの一時コードの内、X医師にはT01, T02, T03, …を割り振り、Y医師にはT01, T02, T03, …を割り振り、Z医師にはT01, T02, T03, …を割り振る。

[0111] 割り振られた一時コードは、各医師が持つ個人認証装置1の管理手段1g中の一時コード管理手段20aに格納する。

[0112] また、個人認証装置1は、管理手段1g中の処置コード管理手段に処置コード(A01, A02, A03, …)を備え、薬剤コード管理手段に薬剤コード(B01, T02, T03, …)を備え、入力手段1jから診察で指定した薬剤や処置が指定されると、対応するコードを出力手段1hから記録媒体2(2A, 2B, …)に記録すると共に、同コードを入出力手段1iからサーバ20内のコード管理装置20bに記録する。なお、薬剤コードや処置コードは、一時コードと共に記録媒体2に格納してもよい。

[0113] 異なる医療対象者に対して投薬や処置を行う場合には、各医療対象者の携帯装置2A, 2Bに対して異なる一時コードT01, T02を設定し、これによって、医療対象者と投薬や処置の識別を行う。

[0114] また、一時コードは医師等毎に異なるコードが発行されているため、医療対象者や投薬や処置を特定する他、指示した医師も特定することができる。

[0115] 図15では、一時コードをサーバ20側で発行する例を示しているが、一時コードの発行は個人認証装置1側で行うこともできる。図16は一時コードを個人認証装置1側で発行する例を示している。

[0116] 各個人認証装置1は、管理手段1g中の一時コード発行手段においてそれぞれ固有の一時コードを発行し、当該一時コードを出力手段1hから記録媒体2(2A, 2B, …)に記録すると共に、同コードを入出力手段1iからサーバ20内の一時コード管理装置20cに記録する。その他は、前記図15の構成と同様とすることができる。

[0117] 次に、投薬、処置段階120について図17を用いて説明する。記録媒体2には診察段階で設定された一時コード(T01)が設定されている。処置室や点滴に際において、当該処置場所あるいは処置者は個人認証装置1を備え、この個人認証装置1によって前記した様に、指紋センサ1aで検出した指紋とスキャナ1cで読み込んだ指紋照

合用データとを照合手段1bで照合することによって個人認証を行う他、スキャナ1cで読み込んだ一時コードと、サーバ20から送信された一時コードとを照合手段1kで照合することによって、投薬や処置に誤りがないことを確認する。照合手段1kによる照合結果は表示手段1fに表示する。

- [0118] また、投薬や処置の確認は、サーバ20から送られた一時コードを用いる他、一時コードを薬剤の袋やケース、あるいは処置装置の外装にシールやICチップ等の記録媒体により付与しておき、この一時コードをスキャナ1cで読み取るようにしてもよい。
- [0119] なお、記録媒体2に薬剤コードや処置コードを記録する場合には、照合手段1kにおいて一時コードに加えて薬剤コードや処置コードを照合してもよい。これによれば、指定された薬剤や処置の確認をより確実に行うことができる。
- [0120] 次に、調剤段階130について図18を用いて説明する。記録媒体2には診察段階で設定された一時コード(T01)が設定されている。診察において指定された薬剤を調剤する際において、当該調剤場所あるいは調剤を受け付ける窓口は個人認証装置1を備え、この個人認証装置1によって前記した様に、指紋センサ1aで検出した指紋とスキャナ1cで読み込んだ指紋照合用データとを照合手段1bで照合することによって個人認証を行う他、スキャナ1cで読み込んだ一時コードと、サーバ20から送信された一時コードとを照合手段1kで照合することによって、薬剤に誤りがないことを確認して調剤操作を行い、薬剤131を作成する。なお、この薬剤131を収納する袋やケースの外装にシールやICチップ等の記録媒体により付与しておき、個人認証装置1のスキャナ1cで読み取り可能とし、以後の薬剤の配布における確認に利用することができる。
- [0121] 次に、薬剤の窓口での受け渡し段階140について図19を用いて説明する。記録媒体2には診察段階で設定された一時コード(T01)が設定されている。診察で指定された薬剤を窓口で受け渡しする際において、当該受け渡し場所あるいは受け渡しを受け付ける窓口は個人認証装置1を備え、この個人認証装置1によって前記した様に、指紋センサ1aで検出した指紋とスキャナ1cで読み込んだ指紋照合用データとを照合手段1bで照合することによって個人認証を行う他、スキャナ1cで読み込んだ一時コードと、サーバ20から送信された一時コードや調剤された薬剤を収納した袋やケ

ースに付した一時コードとを照合手段1kで照合することによって、薬剤に誤りがないことを確認し、薬剤131の受け渡しを行う。

[0122] なお、記録媒体2に薬剤コードや処置コードを記録する場合には、照合手段1kにおいて一時コードに加えて薬剤コードや処置コードを照合してもよい。これによれば、指定された薬剤や処置の確認をより確実に行うことができる。

[0123] 次に、薬剤の受け取り段階150について図20を用いて説明する。この受け取り段階は、病院等において予め用意された薬剤を、番号を指標として受け取りを行う形態に対応するものである。

[0124] 記録媒体2には診察段階で設定された一時コード(T01)が設定されている。ここでは、診察で指定された薬剤を受け取る際において、用意された薬剤がどの番号の位置に配置されているかを確認する配置位置確認段階150Aと、確認した配置位置に置かれた薬剤を受け取る段階150Bの2段階としている。

[0125] 配置位置確認段階150Aにおいて、当該配置位置確認場所は個人認証装置1を備え、この個人認証装置1によって前記した様に、指紋センサ1aで検出した指紋とスキャナ1cで読み込んだ指紋照合用データとを照合手段1bで照合することによって個人認証を行う他、スキャナ1cで読み込んだ一時コードと、サーバ20から送信された一時コードや調剤された薬剤を収納した袋やケースに付した一時コードとを照合手段1kで照合し、照合が確認されたときには、当該薬剤が格納された位置の番号を表示する。

[0126] ここでは、薬剤の配置の一例として、個別に錠がかけられる収納容器150a内に薬剤を収納する例を示している。

[0127] 利用者は、単に個人認証装置1に携帯装置をかざすことによって薬剤が収納されている容器の番号を知ることができる。

[0128] 次に、薬剤の受け取り段階150Bにおいて、当該受け取り場所は個人認証装置1を備え、この個人認証装置1によって前記した様に、指紋センサ1aで検出した指紋とスキャナ1cで読み込んだ指紋照合用データとを照合手段1bで照合することによって個人認証を行う他、スキャナ1cで読み込んだ一時コードと、サーバ20から送信された一時コードや調剤された薬剤を収納した袋やケースに付した一時コードとを照合手

段1kで照合し、照合が確認されたときには、収納容器150aの錠を解錠し、薬剤131を取り出す。

- [0129] 利用者は、単に個人認証装置1に携帯装置をかざすことによって薬剤を取り出すことができる。
- [0130] なお、記録媒体2に薬剤コードや処置コードを記録する場合には、照合手段1kにおいて一時コードに加えて薬剤コードや処置コードを照合してもよい。
- [0131] 次に、本発明の医療分野における利用例として、利用者の履歴データを本人認証に利用する適用例について説明する。
- [0132] この適用例は、本人認証を、本人の指紋と記録媒体2に格納した指紋照合用データとの照合に加えて、本人の診療に関わる履歴を照合の指標として用いる例である。本人の診療に関わる履歴は本人毎に異なるため、この履歴を照合することで本人であるか否かの照合に利用することができる。
- [0133] 図21では、診療に関わる履歴として本人が利用した診療科の履歴を用いる例を示している。各診療科には個人認証装置1が設けられ、各診療科で診療を行う毎に記録媒体2に診療科コードを格納すると共に、サーバ20に個人毎に診療科コードを記録する。図21では、診療科P01, P05, P07を順に診療した例を示している。
- [0134] 本人認証を行う場合には、個人認証装置1は、前記したと同様に、指紋センサ1aで検出した指紋とスキャナ1cで読み込んだ指紋照合用データとを照合手段1bで照合することによって個人認証を行う他、スキャナ1cで読み込んだ診療科コードの履歴と、サーバ20から送信された診療科コードの履歴とを照合手段1kで照合し、照合が確認されたときには、本人であることを確認する。
- [0135] なお、診療に関わる履歴は、上記した診療科の利用順の他、利用した診療科と時間との組み合わせとしたものを用いてもよい。これによれば、利用する診療科の個数が少ない場合であっても本人認証に利用することができる。
- [0136] 本発明の実施の形態によれば、被認証者は指紋照合用データや識別データや個人情報等の種々の記録情報を読み出す操作について、格別な意識あるいは配慮を払うことなく、単に指紋データを取得するために指紋を指紋センサに接触するだけで個人情報を取得することができる。

- [0137] 本発明の実施の形態によれば、指紋照合を行うために要する指紋照合用データを、カードに記録したりあるいはサーバに格納しておく必要がないため、指紋照合のための装置を簡略化して小型とすることができる。
- [0138] 本発明の実施の形態によれば、記録媒体を搭載する携帯装置は、利用者の指や手首や足首に太さに応じて容易に形成することができる。
- [0139] さらに、本発明の携帯装置は医療分野に適用することで以下のような格別な効果を奏することができる。
- [0140] 医療分野において、通常、医療対象者は身体に不自由な箇所があり、また、年齢においても高齢者や年少者など、十分な意思疎通が期待できない場合が多い。そのため、医療対象者の個人認証を行う際、医療対象者自身に複雑な個人認証操作を要求することは望ましくなく、簡易な操作により個人認証を行うことができる装置が望まれる。
- [0141] 例えば、医療対象者は意識不明や身体を自由に動かせない場合には、本人が暗証番号を入力する等の操作を必要とする認証装置は不適である。また、カードを用いて個人認証を行う場合には、本人がカードを必ずしも管理しているとは限らず、手術等の治療現場では身体に何も身につけずに治療が行われる場合があり、カード等の媒体を所持することはできない。
- [0142] また、医療分野では、診療、点滴、投薬等の、取り違えの防止が強く求められる処置が多く、取り違えの可能性を極力小さくするために常に身につけられることが要求される。
- [0143] 上記のような医療分野という特別な環境において、本発明の個人認証では、カード等の媒体のように所持が困難な状況においても身体に常に身につけることができ、また、故意に付け替えるといったことをしない限り、取り違えるといった事態も生じないという格別な効果を奏することができる。
- [0144] また、簡易な操作によって行うことができ、また、本人でなくとも操作を行うことができるため、個人認証の対象者が意識不明であったり身体を動かせない状況においても、本人による認証操作によらずに操作を行うことができる。

産業上の利用可能性

[0145] 本発明の個人認証装置は、押印やサイン処理に適用することができる他、医療分野に置いても広く適用することができる。

請求の範囲

- [1] 指紋を検出する指紋センサと、被認証者の指又は手首あるいは足首に携帯する携帯装置に搭載される記憶媒体を呼び出し当該記憶媒体に格納される記録情報を読み出すスキャナとを装置本体に一体に備えと共に、
前記指紋センサで検出した被認証者の指の指紋データと、前記スキャナにより前記被認証者の指又は手首あるいは足首に装着された携帯装置の記録媒体から読み出した指紋照合用データとを照合する指紋照合手段とを備え、当該指紋照合により前記記録媒体の所持者と本人との同一性を認証することを特徴とする、個人認証装置。
- [2] 前記携帯装置は、指輪状形状又は腕輪状形状であることを特徴とする、請求項1に記載の個人認証装置。
- [3] 前記指紋センサと前記スキャナは、装置本体上において、指紋センサによる被認証者の検出対象の指紋検出と、被認証者が携帯する携帯装置に搭載される記録媒体の読み出しとを同時に行うことができる位置に配置することを特徴とする、請求項2に記載の個人認証装置。
- [4] 装置本体は表示手段を備え、
前記指紋照合に基づいて、前記スキャナは前記記憶媒体に格納される記録情報から個人情報を読み取って前記表示手段に表示することを特徴とする、請求項1乃至3の何れかに記載の個人認証装置。
- [5] 前記指紋照合に基づいて、前記スキャナは前記記憶媒体に格納される記録情報から個人を特定する識別データを読み取って外部サーバに送り、
外部サーバから当該識別データで特定される個人情報を取り込むことを特徴とする、請求項1乃至4の何れかに記載の個人認証装置。
- [6] 前記指紋照合に基づいて、前記指紋センサが検出した指紋データを外部サーバに送り、
外部サーバから指紋データで特定される個人情報を取り込むことを特徴とする、請求項1乃至4の何れかに記載の個人認証装置。
- [7] 請求項1乃至4の何れかに記載の個人認証装置と、印章データを出力する電子押印

装置とを備え、

前記個人認証装置は、前記指紋照合に基づいて、スキャナにより前記記憶媒体に格納される記録情報から印章データを読み取って電子押印装置に送り、

前記電子押印装置は、当該読み取った印章データの外部装置への書き込み及び読み出しを行うことを特徴とする、個人認証装置を備えるシステム。

[8] 装置本体に表示手段を備え、

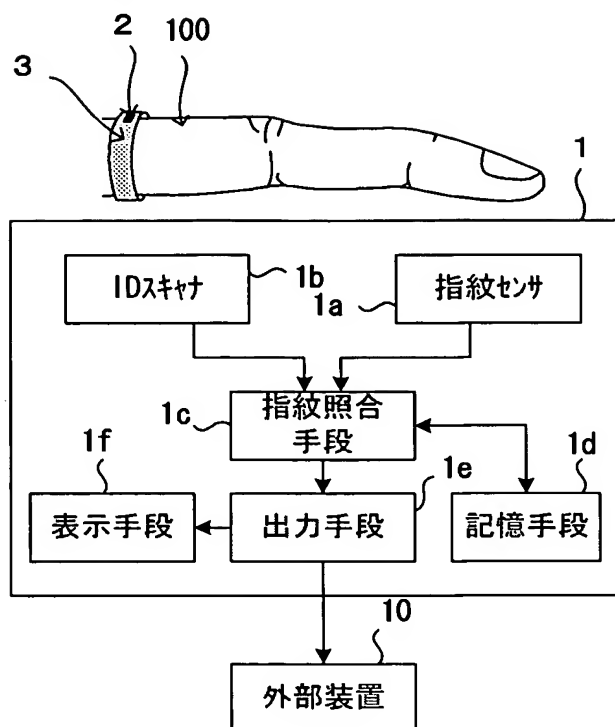
前記記録媒体から読み取った印章データ及び／又は外部装置から読み出した印章データを前記表示手段に表示することを特徴とする、請求項7に記載の個人認証装置。

[9] 請求項1乃至3何れかに記載の個人認証装置と、認証データの照合により解錠する錠装置とを備え、

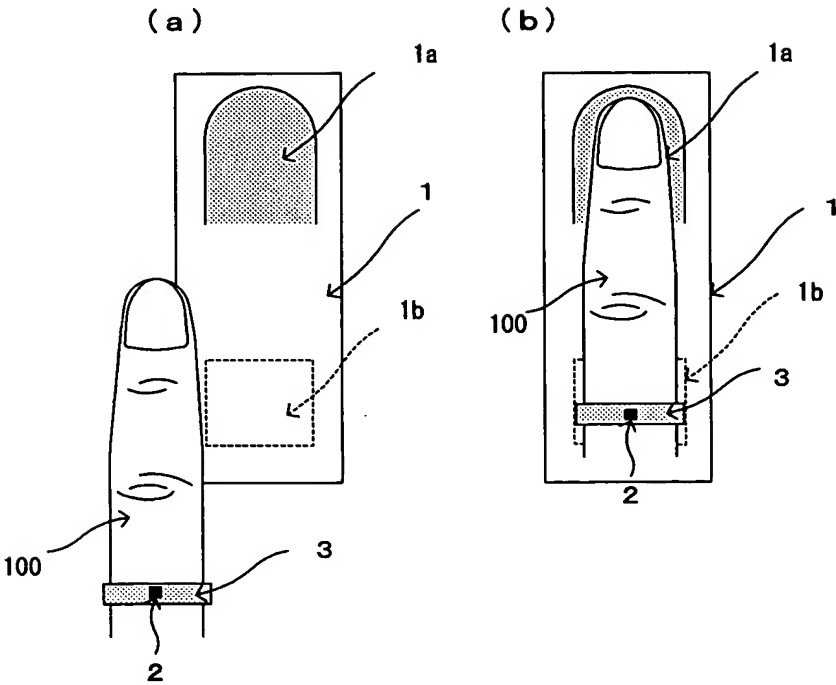
前記個人認証装置は、前記指紋照合に基づいて、スキャナにより前記記憶媒体に格納される記録情報から認証データを読み取って錠装置に送り、

前記錠装置は、前記読み取った認証データと予め記憶する認証データとの照合により解錠することを特徴とする、個人認証装置を備えるシステム。

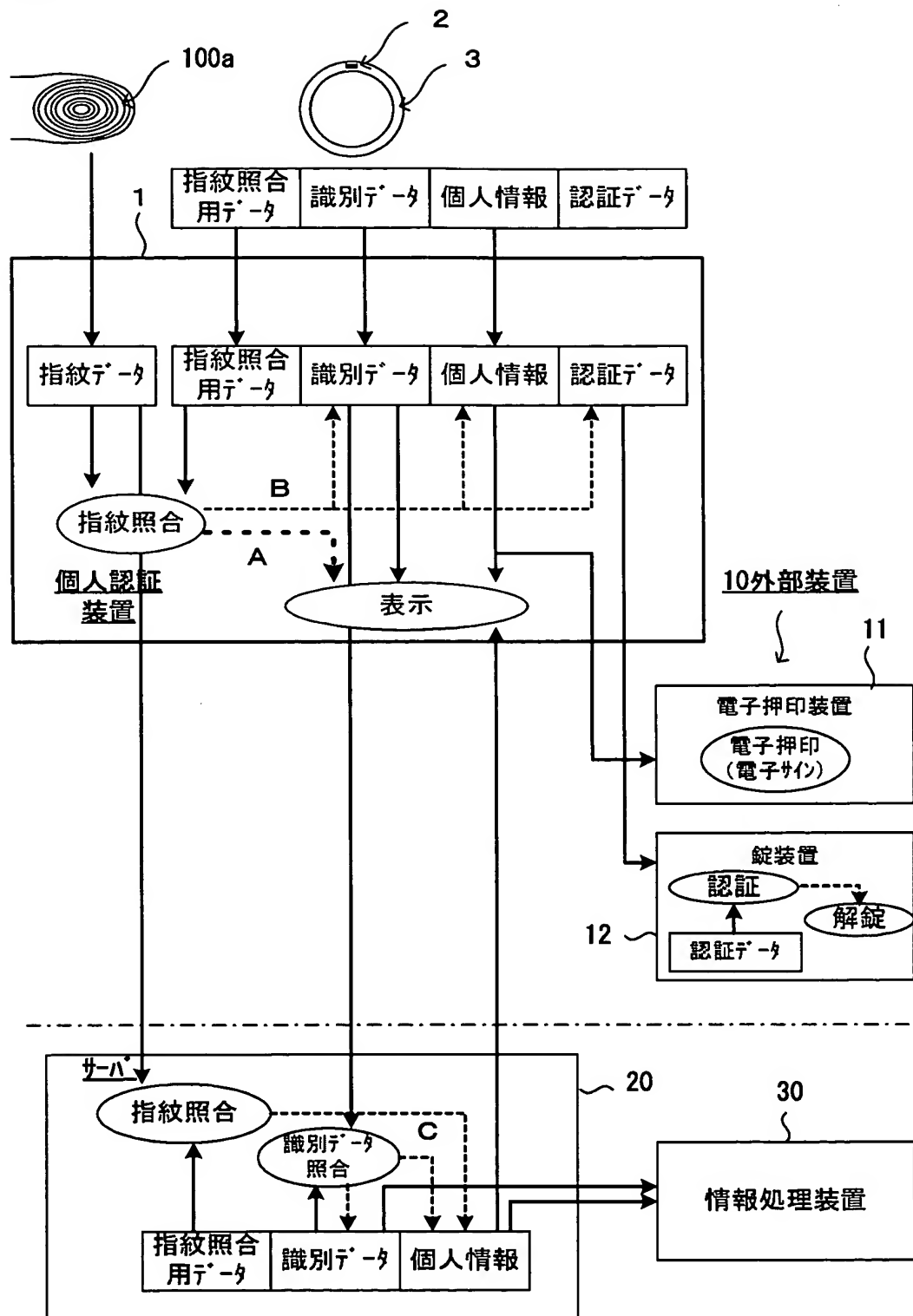
[図1]



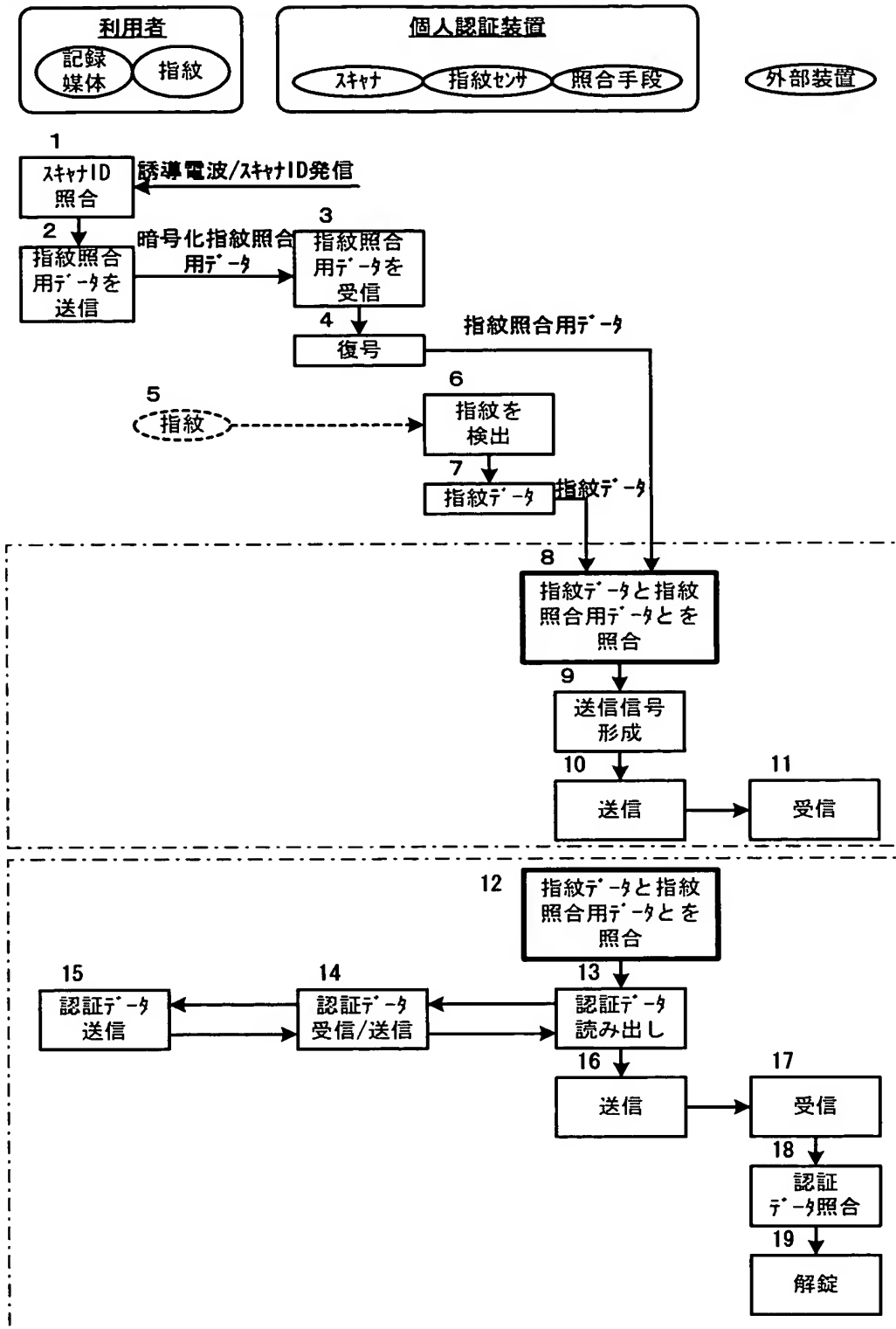
[図2]



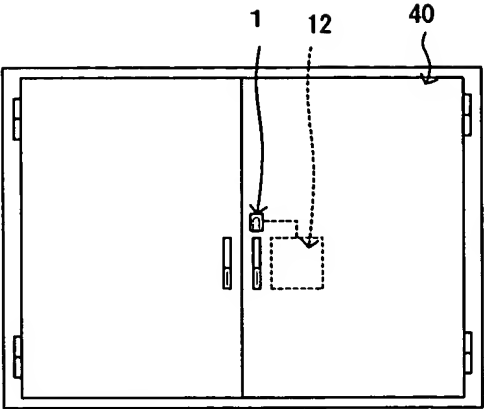
[図3]



[図4]



[図5]



```

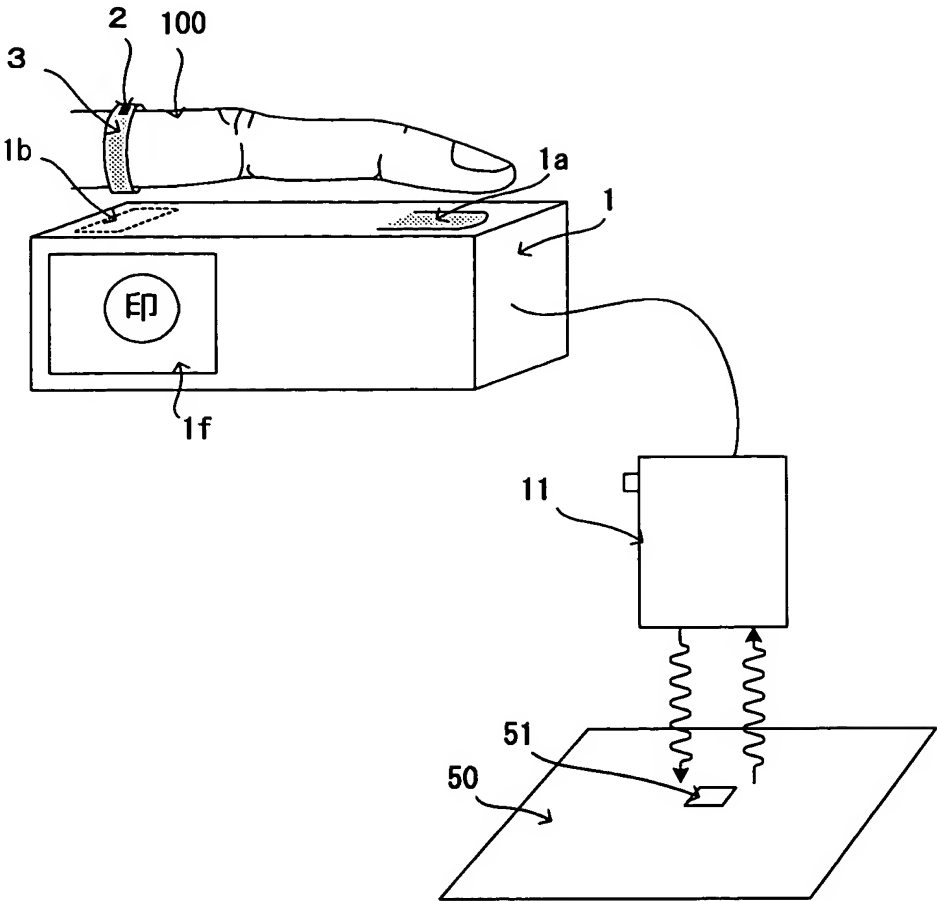
graph TD
    subgraph User [利用者]
        direction TB
        U1[記録媒体]
        U2[指紋]
    end

    subgraph Device [個人認証装置]
        direction TB
        D1[スキャナ]
        D2[指紋センサ]
        D3[照合手段]
        D4[送受信手段]
    end

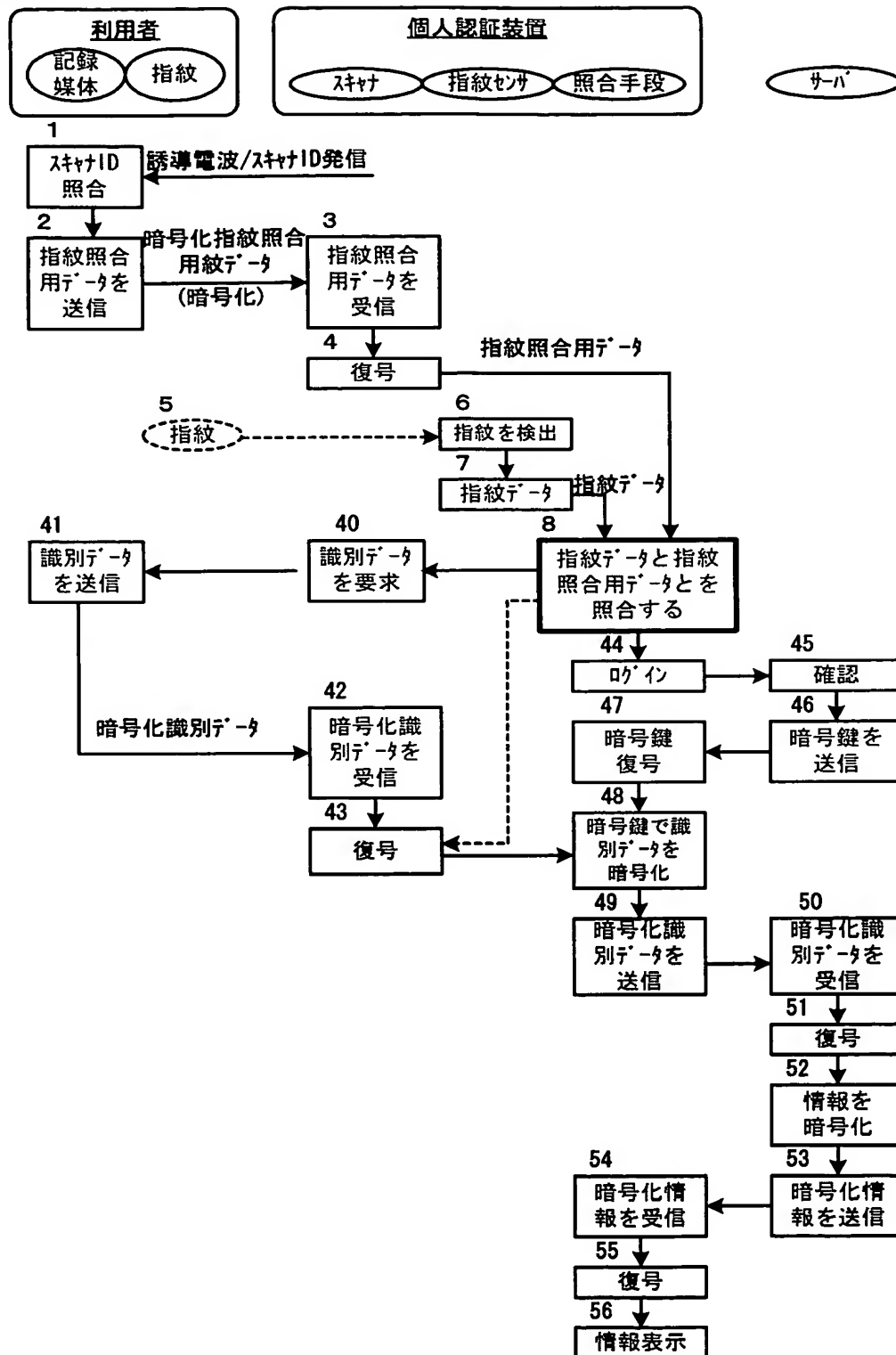
    subgraph Paper [電子押印装置]
        direction TB
        P1[押印用紙  
(無線タグ)]
    end

    1[1 スキャナID照合] -- "誘導電波/スキャナID発信" --> 2[2 指紋照合用データを送信]
    2 -- "暗号化指紋照合用データ (暗号化)" --> 3[3 指紋照合用データを受信]
    3 -- "復号" --> 4[4 指紋照合用データ]
    5[5 指紋] -.-> 6[6 指紋を検出]
    6 -- "指紋データ" --> 7[7 指紋データ]
    4 -- "指紋照合用データ" --> 8[8 指紋データと指紋照合用データとを照合]
    7 -- "指紋データ" --> 8
    8 -.-> 23[23 復号]
    8 -.-> 26[26 電子印章データを受信]
    21[21 電子印章データを送信] -- "暗号化された電子印章データ" --> 22[22 暗号化電子印章データを受信]
    22 -- "復号" --> 23
    23 -- "電子印章データを送信" --> 24[24 電子印章データを送信]
    24 -- "電子印章データを表示" --> 25[25 電子印章データを表示]
    24 -- "電子印章データを受信" --> 26
    26 -- "電子印章データを書込む" --> 27[27 電子印章データを書込む]
    27 -- "電子印章データを記録" --> 28[28 電子印章データを記録]
    28 -- "電子印章データを読み取る" --> 29[29 電子印章データを読み取る]
    29 -- "電子印章データを表示" --> 30[30 電子印章データを表示]
  
```

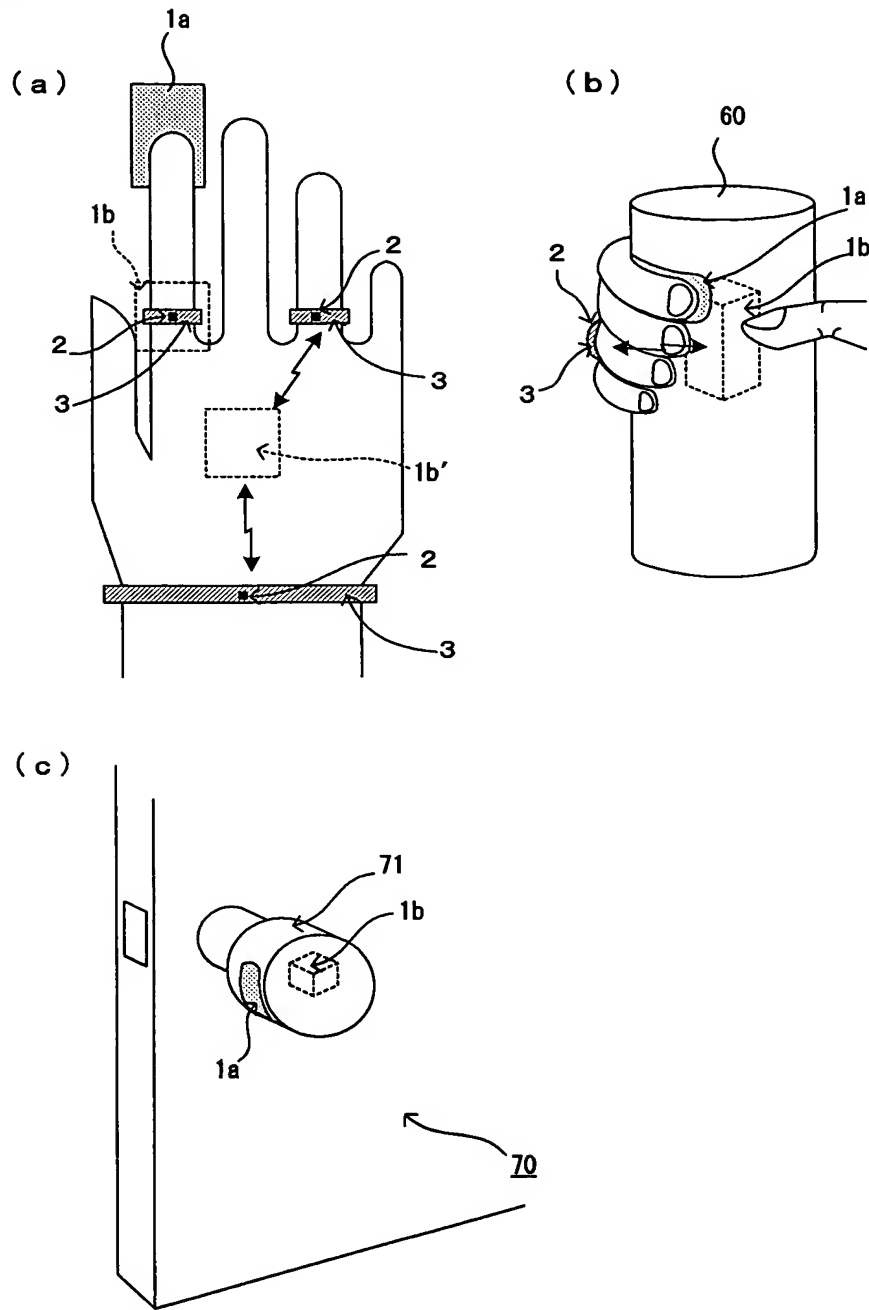
[図7]



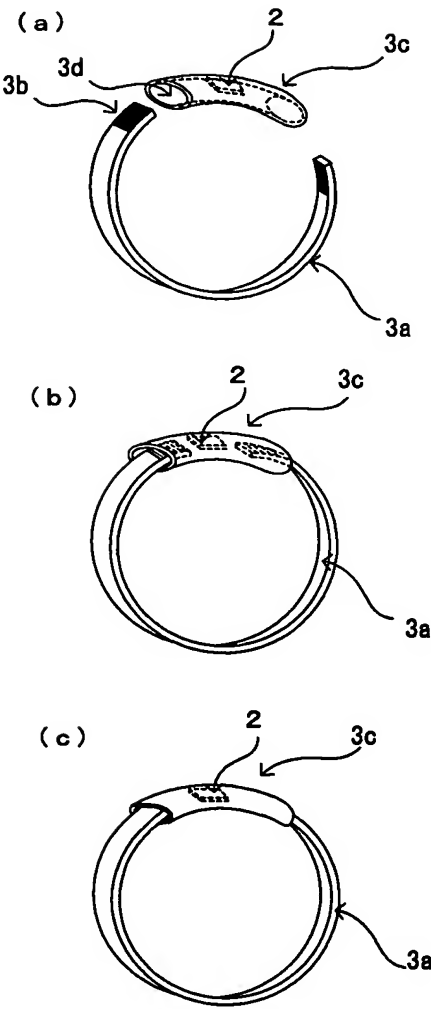
[図8]



[図9]

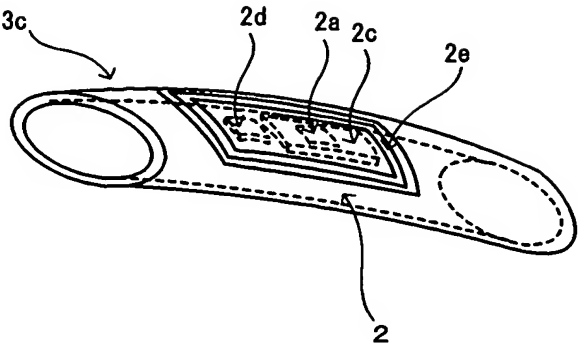


[図10]

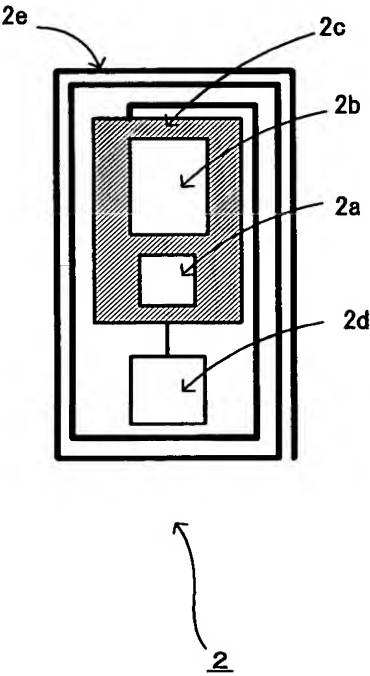


[図11]

(a)

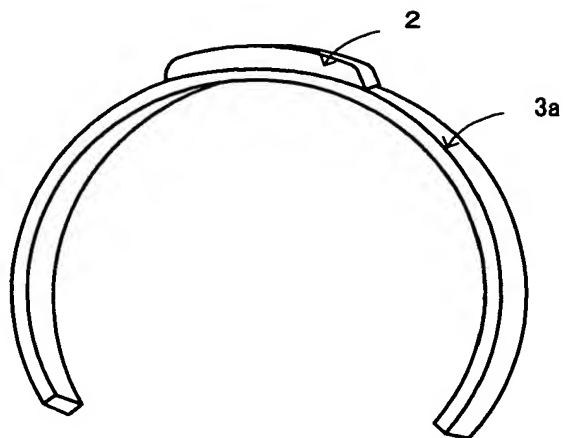


(b)

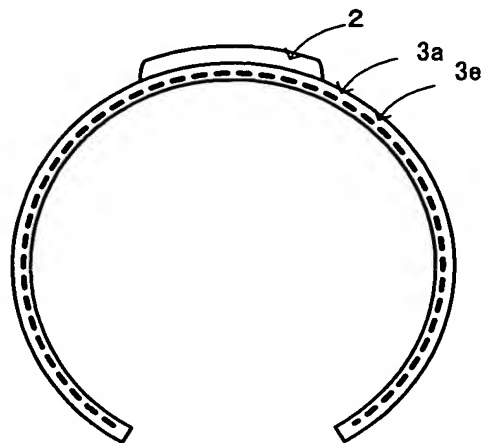


[図12]

(a)

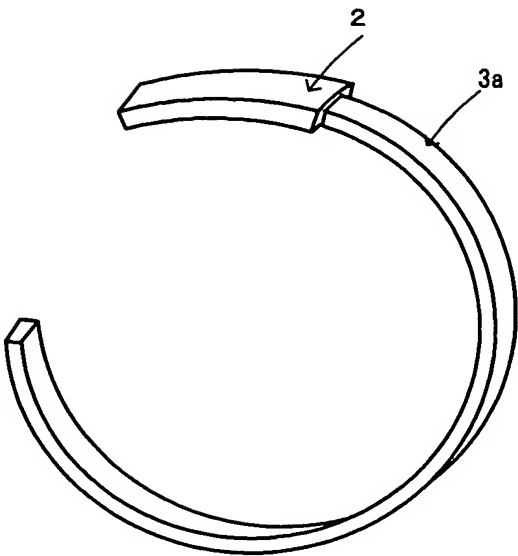


(b)

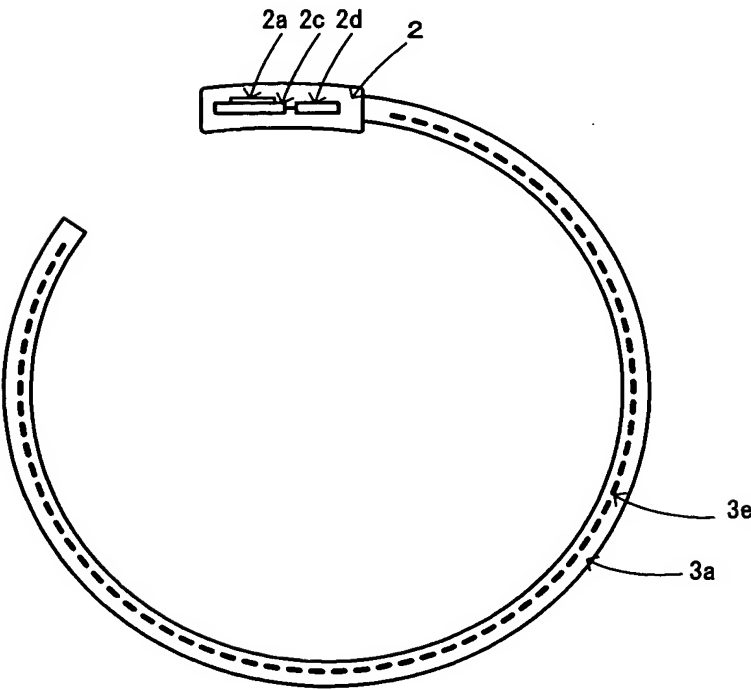


[図13]

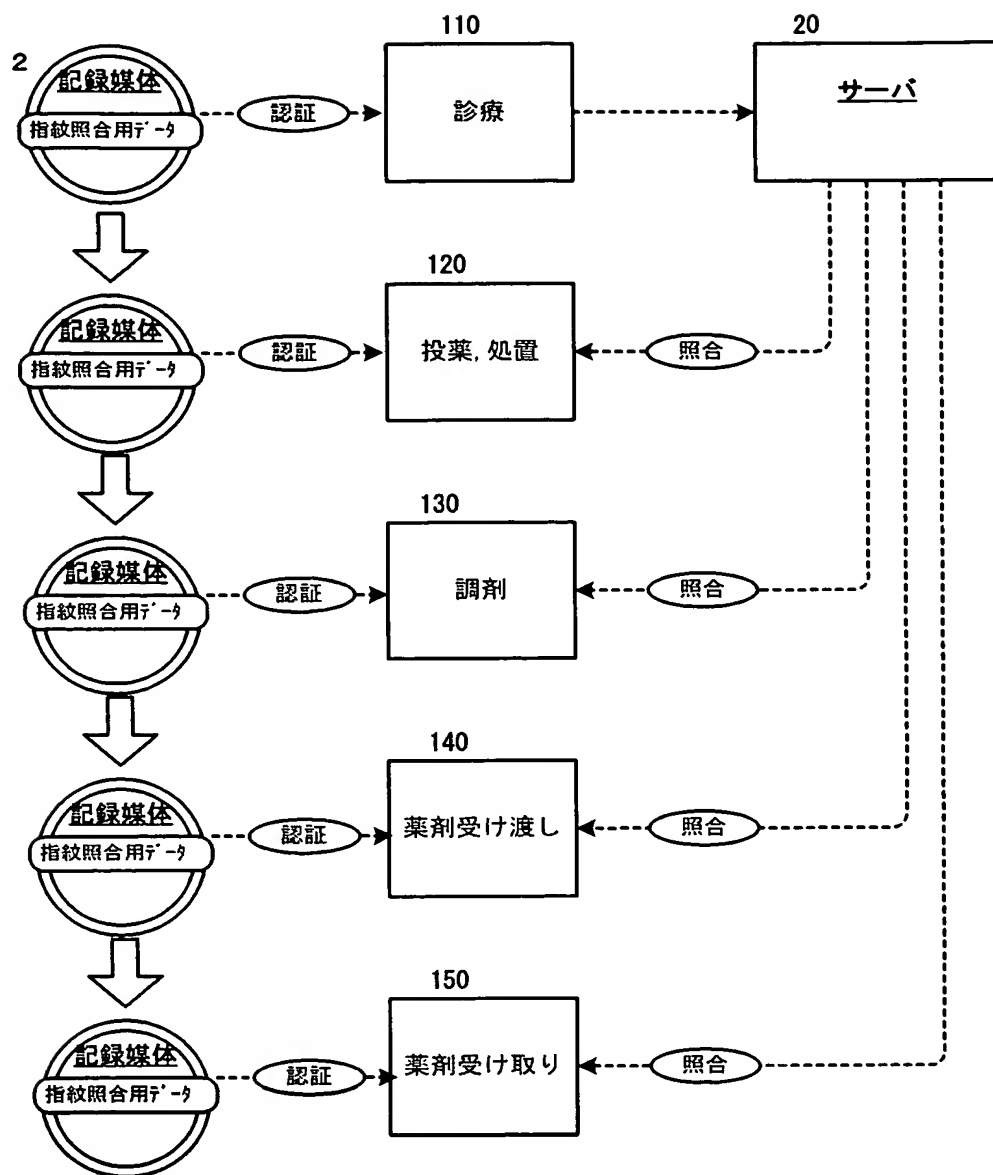
(a)



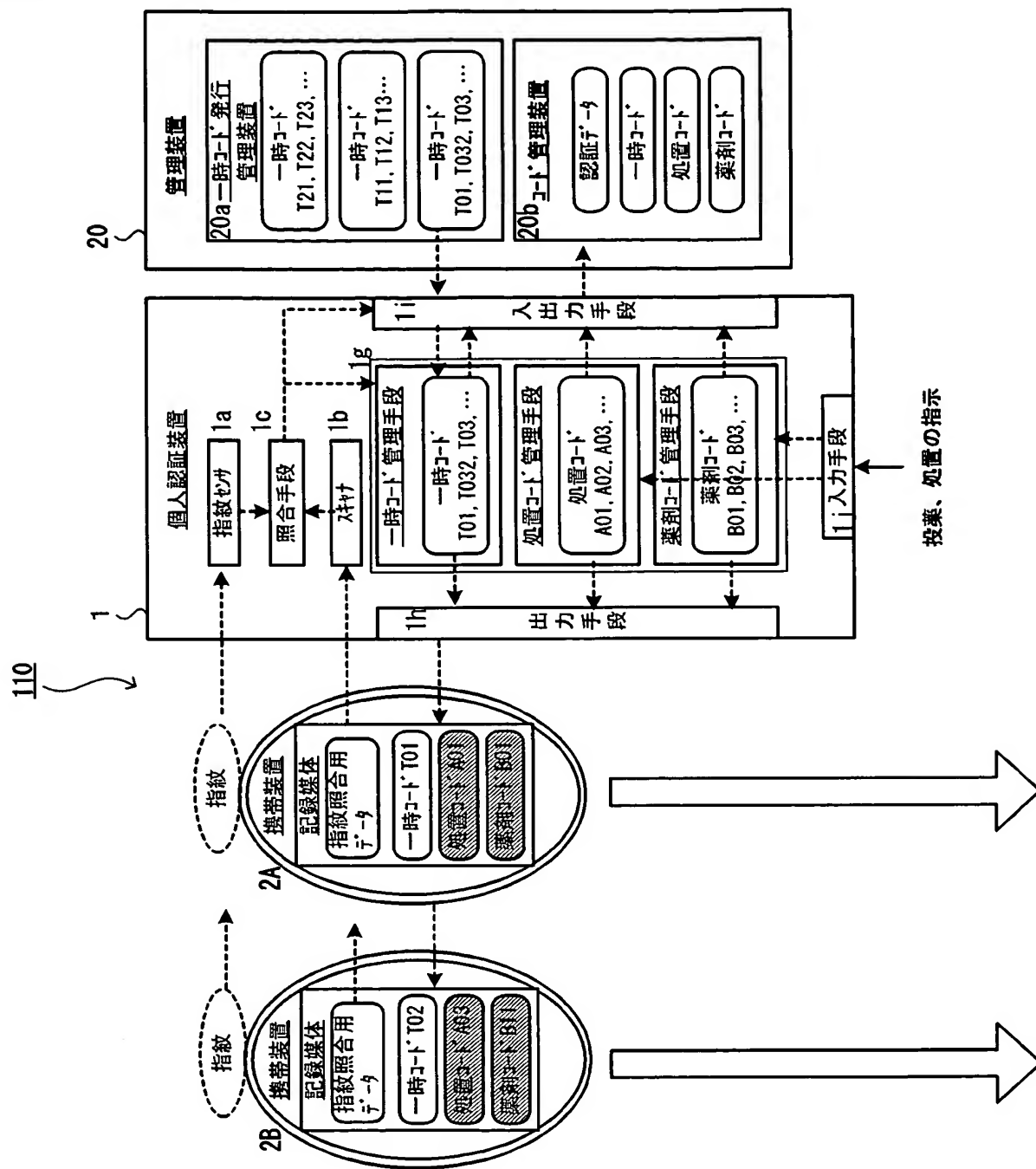
(b)



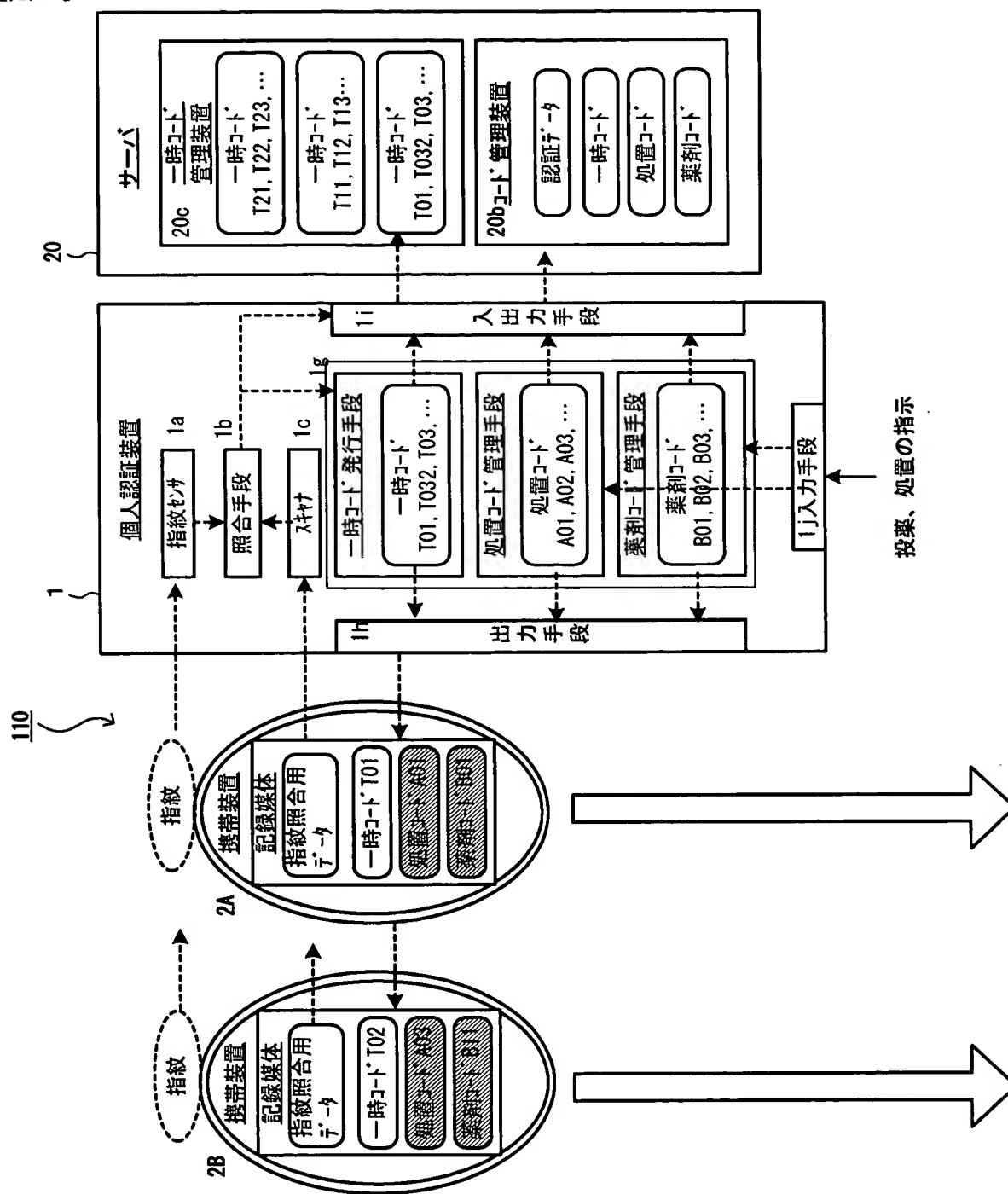
[図14]



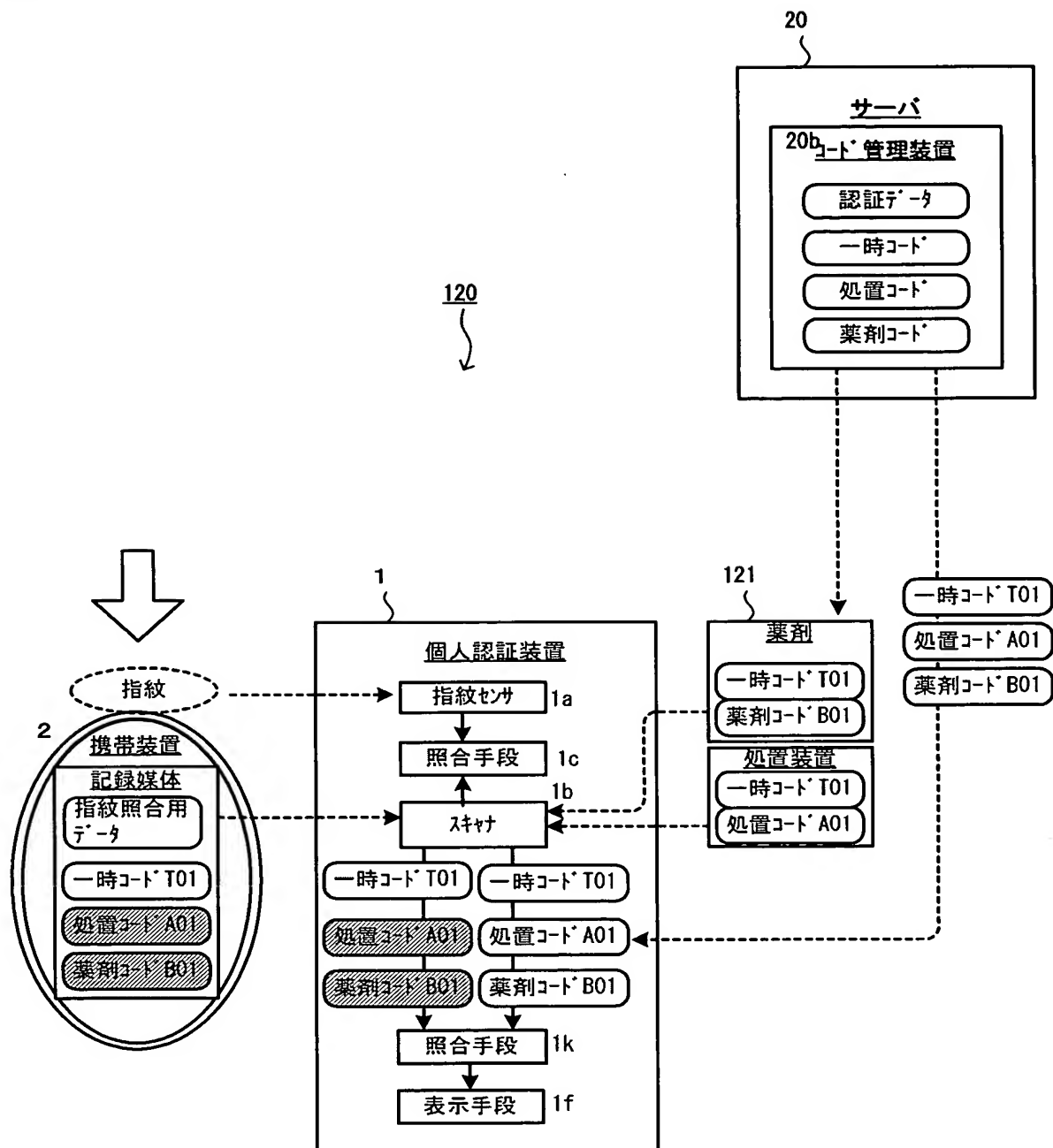
[図15]



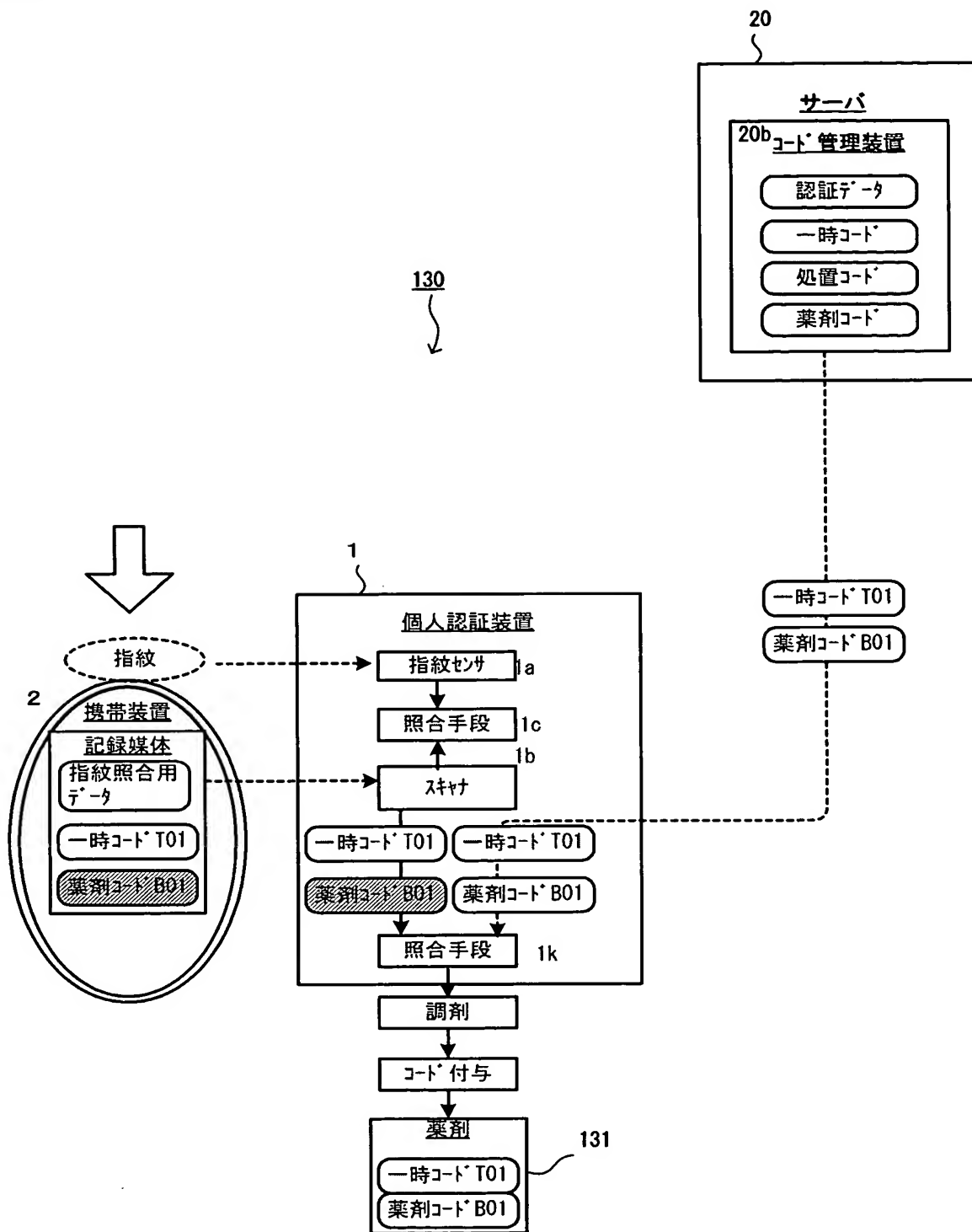
[図16]



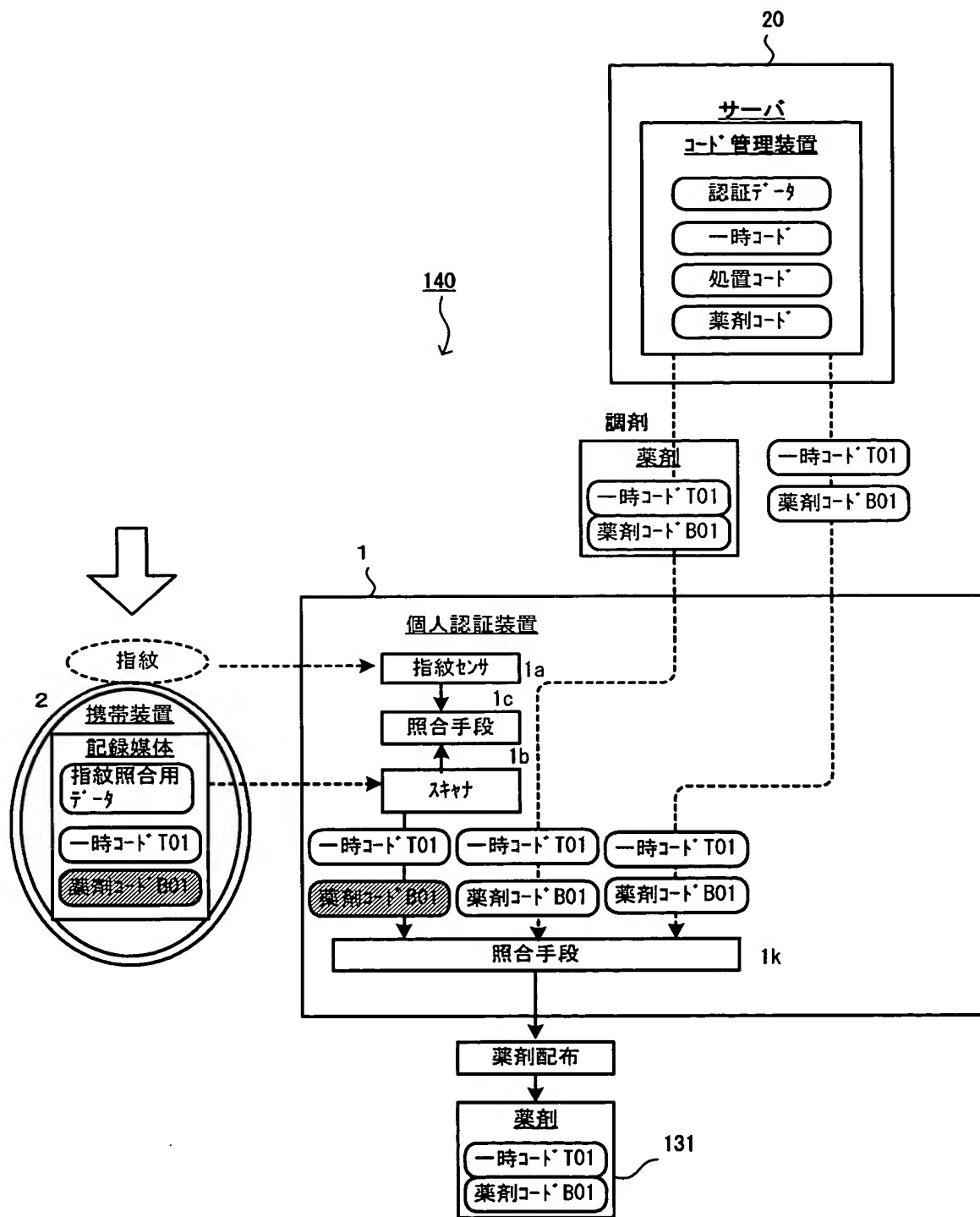
[図17]



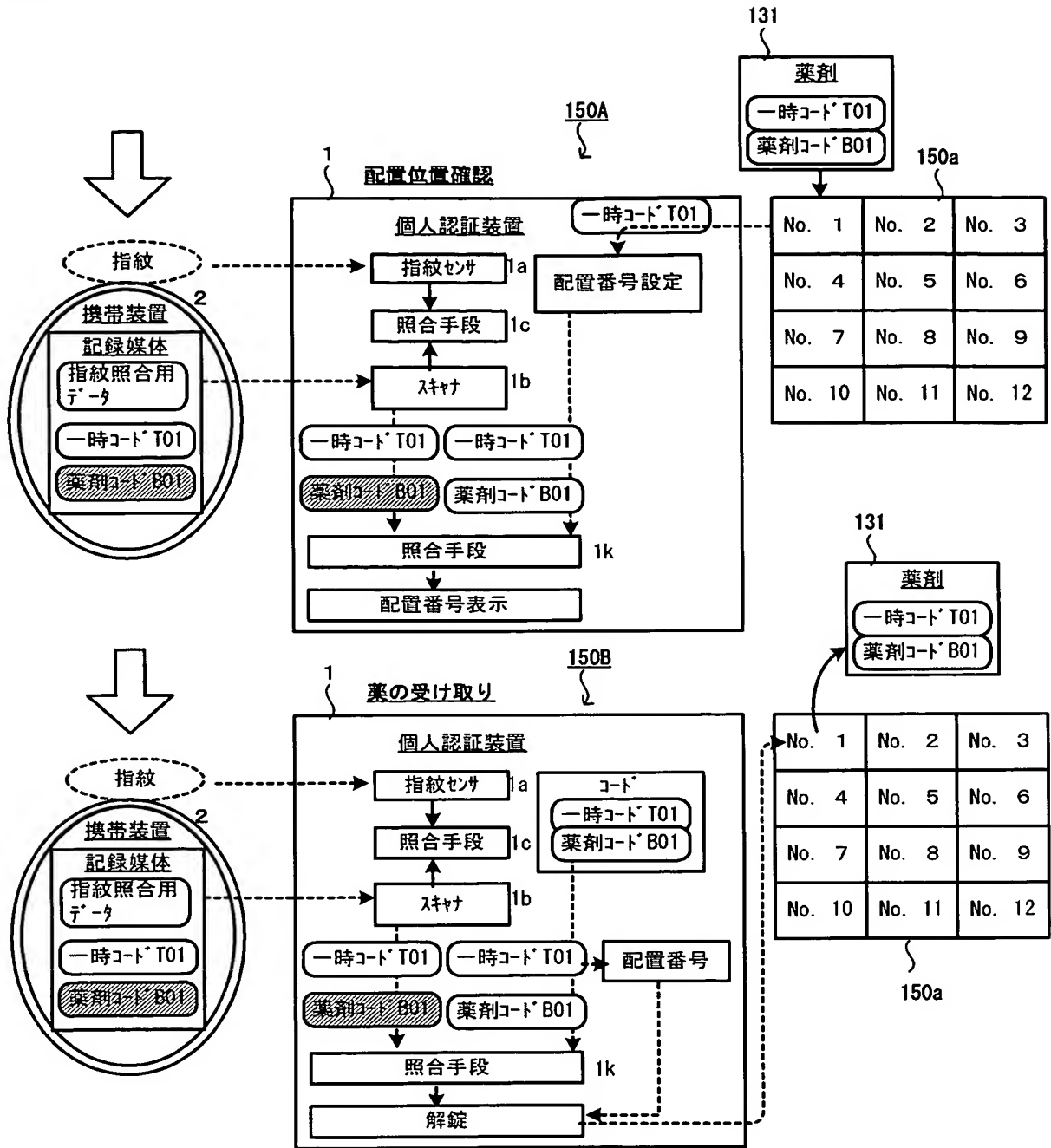
[図18]



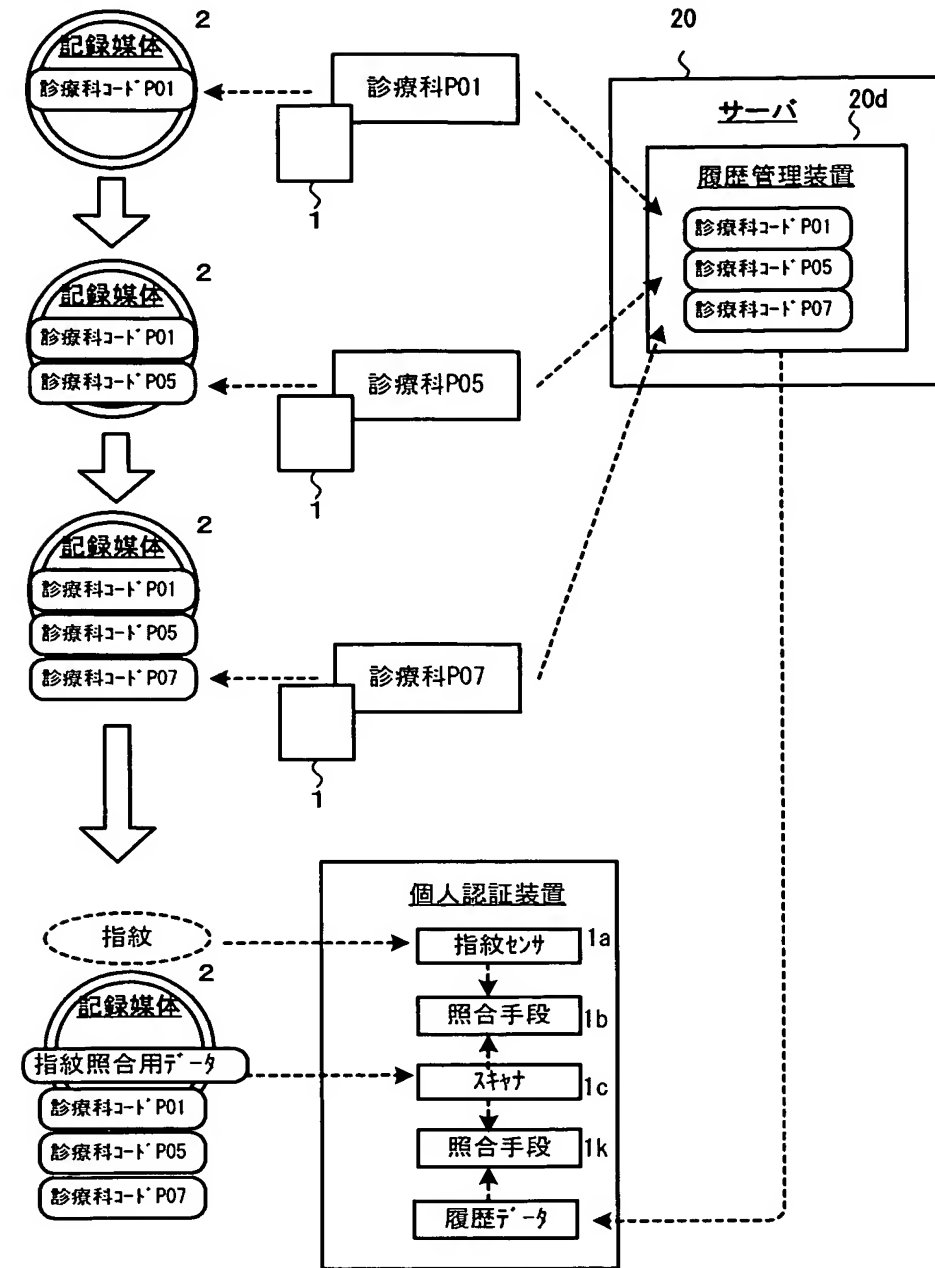
[図19]



[図20]



[図21]



[図22]

